

4 ファイアウォール機能の設定方法

本章では、ファイアウォール機能の設定方法について説明します。

Management Consoleについて

ここでは、設定管理ツールManagement Consoleへの接続方法とその画面構成について説明します。

Management Consoleの接続

管理クライアントのウェブブラウザを使用して、Express5800/SG300のManagement Consoleへ接続します。なお、ウェブブラウザは、Microsoft Internet Explorer 6.0 SP1（日本語版・Windows版）以上を使用することを推奨します。



Management Consoleには必ず内部ネットワークの管理クライアントから接続するようにしてください。



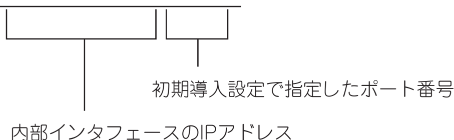
ブラウザが以下のように設定されていることを確認してください。

- JavaScriptを有効にすること
- Cookieを受け入れること

上記のように設定されていないとManagement Consoleが正常に動作しません。

1. Webブラウザを起動し、URLにExpress5800/SG300の内側（管理クライアントが設置されているネットワーク側）のインタフェースのIPアドレスと、初期導入設定ツールで設定したポート番号を指定する。

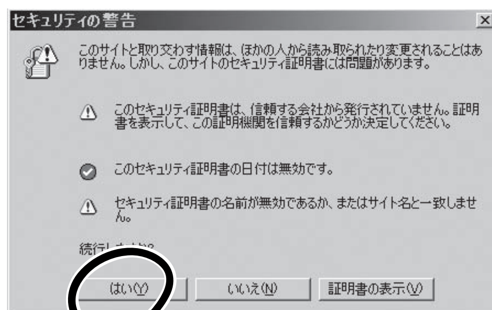
   例） https://192.168.1.126:18000/



   接続すると、セキュリティの警告が表示されます。

2. ［はい］をクリックする。

   ネットワークパスワードの入力画面が表示されます。



セキュリティの警告画面

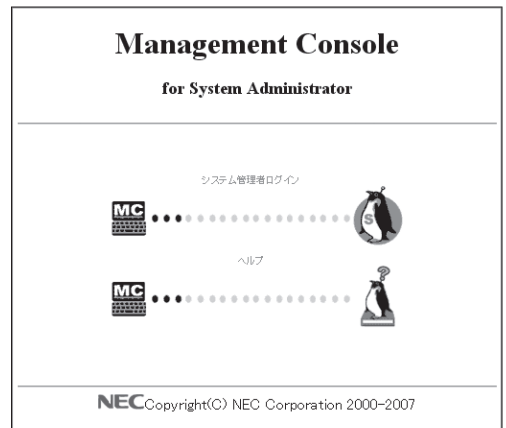
3. 初期導入設定ツールで設定した管理者アカウント名(ユーザ名)とパスワードを入力する。

   接続に成功すると、Management Consoleのログイン画面が表示されます。

パスワードの入力画面

4. [システム管理者ログイン]をクリックする。

   Management Consoleのトップ画面が表示されます。



Management Consoleのログイン画面

Management Consoleのトップ画面

管理者はManagement Consoleのトップ画面から各メニューを選択して、Express5800/SG300の設定と管理を行います。各メニューを以下に示します。



Management Consoleのトップ画面

- **基本設定** .... ネットワークインタフェースのアドレスなど、システムの基本的な設定を行います。
- **ファイアウォール** .... アクセス制御のルール定義など、ファイアウォール機能に関する設定と管理を行います。
- **ディスク** .... ディスクの一覧表示や使用量などの確認を行います。
- **サービス** .... オプション製品をインストールしている場合に、そのオプション製品のサービスの起動/停止を行います。
- **パッケージ** .... インストールされているパッケージの情報の確認と、オプション製品のインストールを行います。
- **システムの管理** .... システムの停止/再起動やシステムの状態の確認、およびシステムログの管理などを行います。
- **Management Console** .... Management Consoleのリモートメンテナンス機能に関する設定を行います。

以降、「ファイアウォール」メニューの設定について詳細に説明します。その他のメニューについてはManagement Consoleのヘルプを参照してください。



- **画面上の各ボタンは一度だけクリックしてください。二度以上連続してクリックすると正しく画面が遷移しないことがあります。**
- **ブラウザの戻るボタンやキーボードのショートカットによる戻る機能は使用しないでください。**

かんたん設定ウィザード

Express5800/SG300のファイアウォール機能を利用するには、はじめに「かんたん設定ウィザード」を利用して、ネットワーク構成の選択やフィルタリングの設定などを行う必要があります。
ネットワーク環境が複雑な構成でないときには、このかんたん設定ウィザードに従って設定するだけで、ファイアウォール機能を利用することができます。
かんたん設定ウィザードで設定できる項目を以下に示します。



かんたん設定ウィザードから設定できる内容は、詳細設定メニューの「ルール設定」からも設定することができます。詳細設定メニューの「ルール設定」から設定を行うと、かんたん設定ウィザードで設定できる項目に加えて、通信ログを記録するように設定することや、コメントを登録することができます。
かんたん設定ウィザードで設定したルールについて、通信ログを記録する場合やコメントを登録する場合は、詳細設定メニューの「ルール設定」から編集することができます。
なお、かんたん設定ウィザードから、通信ログの記録やコメント登録を設定したルールの再登録を行うと、記録とコメントの設定がクリアされるので注意してください。

設定内容の確認 .... すでにかんたん設定ウィザードを使って設定している場合は、設定内容を表示します。

ネットワーク構成の選択 .... Express5800/SG300を導入するネットワークにDMZを構築するかどうか、ブリッジ機能を使うかどうかを選択します。

ネットワークインタフェースの選択 .... Express5800/SG300のインタフェースの設定を行います。

公開サーバの設定 .... 外部ネットワークに公開するサーバ群のIPアドレスやポート番号などの設定を行います。

外部サービスの利用の設定 .... 内部ネットワークから外部ネットワークの各種サービスを利用する場合のフィルタリング設定を行います。

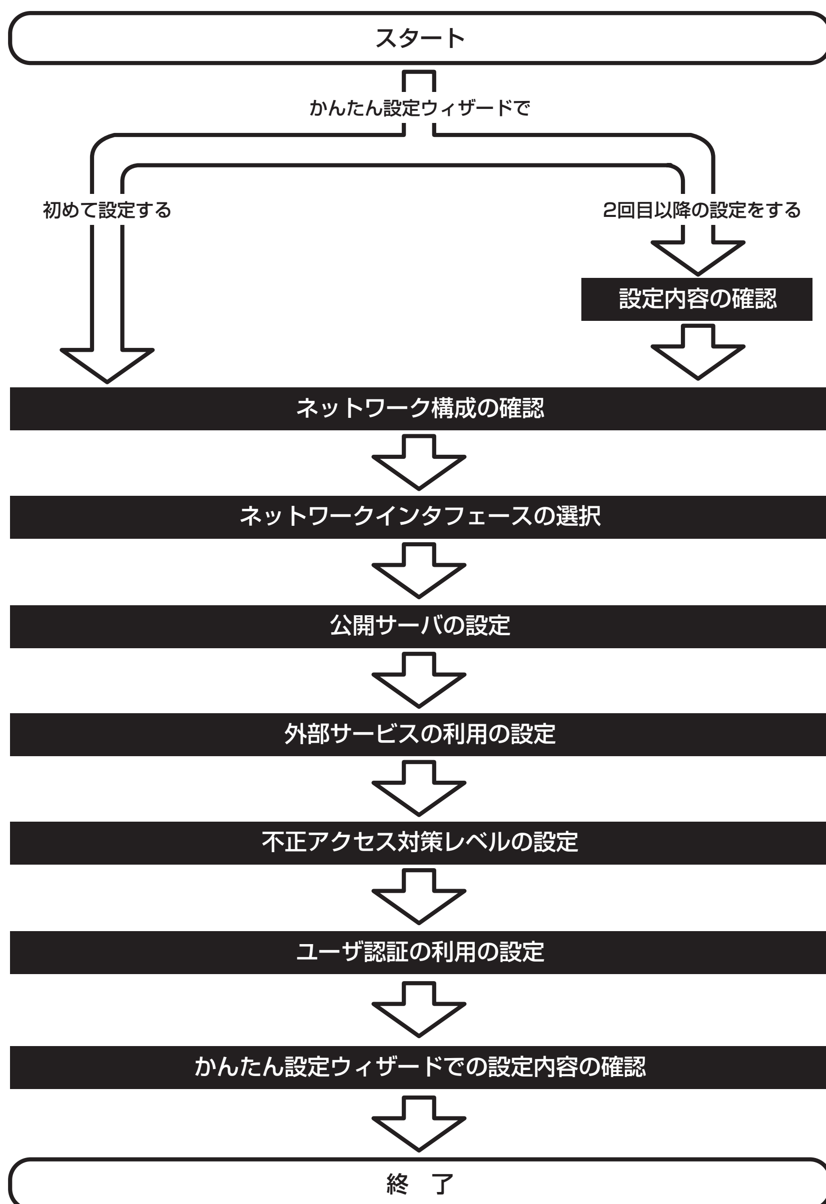
不正アクセス対策レベルの設定 .... 外部ネットワークからのアクセス制御のレベルを設定します。

ユーザ認証の利用の設定 .... ユーザ認証機能についての設定を行います。

設定内容の確認 .... かんたん設定ウィザードで設定した内容を確認します。

設定作業の流れ

かんたん設定ウィザードでは、以下のような流れで設定作業を行います。



設定内容の確認

かんたん設定ウィザードですでに設定を行っている場合、現在の設定状況の確認が行えます。ただしセットアップ直後など、一度もかんたん設定ウィザードを利用したことがない場合には、確認画面は表示されずネットワーク構成の選択画面に進みます。

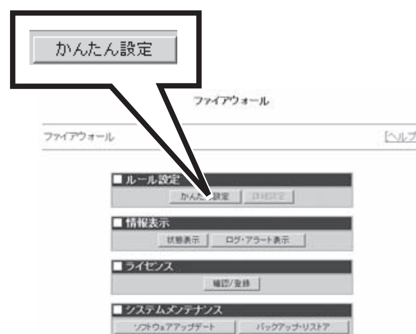
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[かんたん設定]をクリックする。

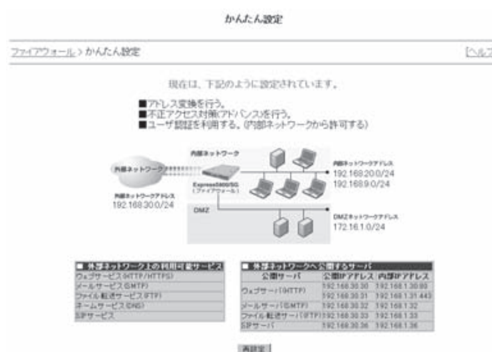
   設定内容確認画面が表示されます。



ファイアウォールメニュー画面

3. 設定内容確認画面から以下の項目を確認する。

   - NAT/NAPTによるアドレス変換の設定の有無
     Express5800/SG300がアドレス変換を行うかどうか表示します。
     ブリッジ構成の場合は、「ブリッジ機能を利用する」と表示されます。
   - 不正アクセス対策レベル
     不正アクセス対策レベルを表示します。
   - ユーザ認証
     ユーザ認証を利用するかどうかを表示します。
   - ネットワーク構成
     ネットワークの構成、外部ネットワークアドレス、内部ネットワークアドレス、DMZネットワークアドレスを図で表示します。
   - 外部ネットワーク上の利用可能サービス
     内部ネットワークから利用できる外部ネットワーク上のサービスを一覧表示します。
   - 外部ネットワークへ公開するサーバ
     外部ネットワークから利用できる内部ネットワーク上のサーバと、そのサーバの公開IPアドレス、内部IPアドレスを一覧表示します。



設定内容確認画面

4. [再設定]をクリックする。

   ネットワーク構成の選択画面が表示され、ネットワーク構成の選択に進みます。

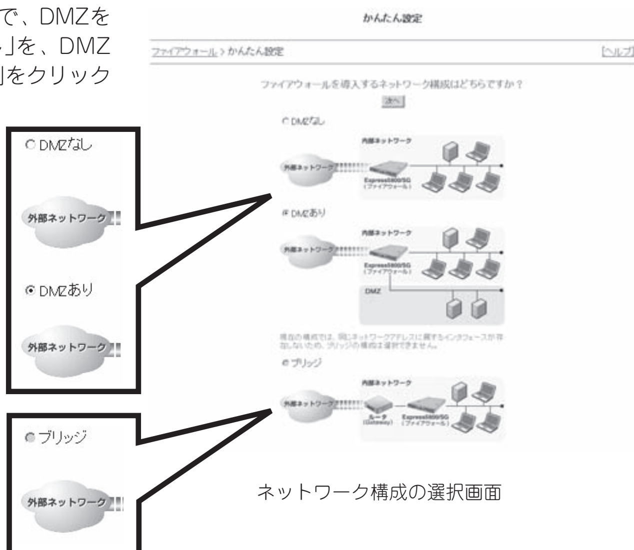
ネットワーク構成の選択

ネットワーク構成の選択では、Express5800/SG300を導入するネットワークの構成として、DMZを利用するかどうかを選択します。
ここで、DMZを利用する構成を選択した場合は、Express5800/SG300に接続されたネットワークは、「外部」、「内部」および「DMZ」に分類されます。DMZを利用しない構成やブリッジ構成を選択した場合は、「外部」と「内部」に分類されます。



- 初めてかんたん設定ウィザードを利用するときは、「ファイアウォール」メニューの「ルール設定」から[かんたん設定]をクリックするとネットワーク構成の選択に進みます。
- 2回目以降の設定の場合は設定内容の確認画面から[再設定]をクリックすると、ネットワーク構成の選択に進みます。

1. ネットワーク構成の選択画面で、DMZを利用しない場合は「DMZなし」を、DMZを利用する場合は「DMZあり」をクリックする。
   Express5800/SGをブリッジとして接続する場合は、［ブリッジ］をクリックする。



ネットワーク構成の選択画面

2. ［次へ］をクリックする。

   インタフェース選択画面が表示され、ネットワークインタフェース選択に進みます。



DMZとは、外部へ公開するサーバを設置するために独立させたセグメントのことで、日本語では「非武装地帯」と訳されます。この部分に外部に公開するサーバを設置し、ファイアウォールでアクセス制御をすることで、安全性を高めることができます。

たとえば、外部ネットワークからDMZへのアクセスは許可し、DMZから内部ネットワークへのアクセスは許可しない、というように設定すれば、万一、DMZに設置したサーバが第三者に不正侵入されたとしても、内部ネットワークにはアクセスできないため、被害を最小限にとどめることができます。

ネットワークインタフェースの選択

ネットワーク構築の選択で「DMZなし」、「DMZあり」を選択した場合は、外部ネットワークのインタフェースを選択します。通常は変更する必要はありません。「DMZあり」を選択した場合は、DMZのネットワークインタフェースについても選択します。

ネットワーク構築の選択で「ブリッジ」を選択した場合は、デフォルトゲートウェイとなるルータの内向けインタフェースを確認します。

1. インタフェース選択画面で、外部ネットワークにつなげるネットワークインタフェースをプルダウンメニューより選択する。

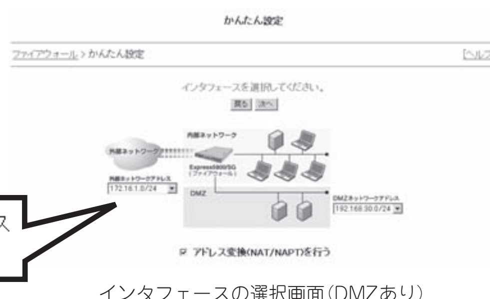


インタフェースの選択画面(DMZなし)



プルダウンメニューに表示されるネットワークインタフェースのIPアドレスは、初期導入設定ツール、またはManagement Consoleの「基本設定」で設定した、ネットワークインタフェースのネットワークアドレスが表示されます。

2. 「DMZあり」を選択している場合は、DMZにつなげるネットワークインタフェースをプルダウンメニューより選択する。



インタフェースの選択画面(DMZあり)

3. インタフェース選択画面で「ブリッジ」を選択している場合は、デフォルトゲートウェイとなるルータの内向けインタフェースのIPアドレスが正しいか確認する。



インタフェースの選択画面(ブリッジ)



ルータ(デフォルトゲートウェイ)のIPアドレスが間違っていると、ブリッジ機能は正しく動作しません。IPアドレスが正しくない場合は、「基本設定」でデフォルトゲートウェイのIPアドレスを再設定してから、再度かんたん設定を行ってください。

4. Express5800/SG300上で、外部に公開するサーバ、内部ネットワークの端末のアドレス変換を行う場合には、「アドレス変換（NAT/NAPT）を行う」のチェックボックスをチェックする。



インタフェースの選択画面（DMZあり）



アドレス変換(NAT/NAPT)とは、内部のネットワークで利用しているIPアドレスが、外部と直接通信できないか、または公開したくないものである場合に、ファイアウォール上でIPアドレスを変換する機能です。たとえば、内部でプライベート(インターネット上のホストとは直接通信できない)IPアドレスを使用している場合に使用します。

ここで、「アドレス変換(NAT/NAPT)を行う」をチェックすると、以降のかんたん設定で公開するサーバを設定する際に、サーバの持つ内部ネットワーク上のIPアドレスとは別に、外部からアクセスするための公開用のIPアドレスを指定できるようになります。外部からこの公開IPアドレスの公開ポートに対してアクセスが行われた場合、ファイアウォール上で宛先IPアドレスを内部IPアドレスに変換します。この機能を「NAT」と呼びます。

また同時に、内部から外部に対してアクセスが行われた場合、ファイアウォール上で送信元IPアドレスをファイアウォールの外部(ネットワークインタフェースに繋がる)IPアドレスに変換します。この機能を「NAPT(またはIPマスカレード)」と呼びます。

5. ［次へ］をクリックする。

ウェブサーバ公開の設定画面が表示され、ウェブサーバの設定に進みます。



［戻る］をクリックすると、ネットワーク構成の選択画面に戻ります。

公開サーバの設定

外部ネットワークに公開するサーバの設定を行います。設定するサーバを以下に示します。

- ウェブサーバ
- メールサーバ
- ファイル転送サーバ
- ネームサーバ
- SIPサーバ
- その他のサーバ群

ウェブサーバの設定

ウェブサーバの設定では、外部ネットワークに公開するウェブサーバのIPアドレスやポート番号などを登録します。



設定するウェブサーバを、不正アクセス対策や詳細設定メニュー(サーバ公開ルール)で設定するウェブ専用フィルタ機能(外→内)の対象とする場合、該当のウェブサーバは80番ポートである必要があります。80番ポート以外を使用したウェブサーバはウェブ専用フィルタ(外→内)の対象になりません。

1. 外部ネットワークへ公開するウェブサーバの有無を選択する。
   - 公開するウェブサーバ(HTTP)はない
     公開するウェブサーバがない場合は、このラジオボタンをクリックし、手順5に進みます。
   - 公開するウェブサーバ(HTTP)はある
     公開するウェブサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

ウェブサーバ公開の設定画面

○ 公開するウェブサーバ(HTTP)はない
◉ 公開するウェブサーバ(HTTP)はある

2. 「公開IPアドレス」に公開するウェブサーバのIPアドレスを入力し、右端のテキストボックスにポート番号を入力する。

公開IPアドレス	
192.168.30.1	443
192.168.30.2	80
	80

ウェブサーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力し、右端のテキストボックスにポート番号を入力する。



ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

ウェブサーバ公開の設定画面



Express5800/SG300の外部インタフェースのIPアドレスを公開アドレスとして使用することもできますが、ポート番号がユーザ認証ウェブ(112ページ参照)と重複しないよう注意してください。「セキュリティ保護」をチェックした場合、ユーザ認証ウェブのデフォルトのポート番号と同じ443番になることに注意してください。

4. 暗号化して通信を行うHTTPS通信を利用する場合には、「セキュリティで保護」のチェックボックスにチェックする。



- 複数台のウェブサーバを公開する場合は、同様に設定を行ってください。
- かんたん設定ウィザードからは、外部に公開するウェブサーバとして3台までしか設定することができません。もし、4台以上のウェブサーバを設定するときには、「その他のサーバ」として設定するか、156ページの「サーバ公開ルール」および121ページの「サイト共通ルール」を参照してルールを追加してください。

ウェブサーバ公開の設定画面

5. [次へ]をクリックする。

メールサーバ公開の設定画面が表示され、メールサーバの設定に進みます。



[戻る]をクリックすると、インタフェース選択画面に戻ります。

メールサーバの設定

メールサーバの設定では、外部ネットワークに公開するメールサーバのIPアドレスを登録します。

1. 外部ネットワークへ公開するメールサーバの有無を選択する。

   ● 公開するメールサーバ(SMTP)はない
   公開するメールサーバがない場合は、このラジオボタンをクリックし、手順4に進みます。

   ● 公開するメールサーバ(SMTP)はある
   公開するメールサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

メールサーバ公開の設定画面

2. 「公開IPアドレス」に公開するメールサーバのIPアドレスを入力する。

メールサーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。



ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

メールサーバ公開の設定画面



かんたん設定ウィザードからは、外部に公開するメールサーバとして1台までしか設定することができません。もし、2台以上のメールサーバを設定するときには、「その他のサーバ」として設定するか、156ページの「サーバ公開ルール」および121ページの「サイト共通ルール」を参照してルールを追加してください。

4. ［次へ］をクリックする。

ファイル転送サーバ公開の設定画面が表示され、ファイル転送サーバの設定に進みます。

 ヒント

［戻る］をクリックすると、ウェブサーバ公開の設定画面に戻ります。

ファイル転送サーバの設定

ファイル転送サーバの設定では、外部ネットワークに公開するファイル転送サーバのIPアドレスを登録します。

1. 外部ネットワークへ公開するファイル転送サーバの有無を選択する。
   - 公開するファイル転送サーバ(FTP)はない
     公開するファイル転送サーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - 公開するファイル転送サーバ(FTP)はある
     公開するファイル転送サーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

公開するファイル転送サーバ(FTP)はない
公開するファイル転送サーバ(FTP)はある

ファイル転送サーバ公開の設定画面

2. 「公開IPアドレス」に公開するファイル転送サーバのIPアドレスを入力する。

公開IPアドレス
192.168.30.5

ファイル転送サーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。



ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

ファイル転送サーバ公開の設定画面



かんたん設定ウィザードからは、外部に公開するファイル転送サーバとして1台までしか設定することができません。もし、2台以上のファイル転送サーバを設定するときには、「その他のサーバ」として設定するか、156ページの「サーバ公開ルール」および121ページの「サイト共通ルール」を参照してルールを追加してください。

4. [次へ]をクリックする。

ネームサーバ公開の設定画面が表示され、ネームサーバの設定に進みます。



[戻る]をクリックすると、メールサーバ公開の設定画面に戻ります。

ネームサーバの設定

ネームサーバの設定では、外部ネットワークに公開するネームサーバのIPアドレスを登録します。

1. 外部ネットワークへ公開するネームサーバの有無を選択する。

   - 公開するネームサーバ(DNS)はない
     公開するネームサーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - 公開するネームサーバ(DNS)はある
     公開するネームサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

ネームサーバ公開の設定画面

2. 「公開IPアドレス」に公開するネームサーバのIPアドレスを入力する。

ネームサーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。



ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

ネームサーバ公開の設定画面



かんたん設定ウィザードからは、外部に公開するネームサーバとして1台までしか設定することができません。もし、2台以上のネームサーバを設定するときには、「その他のサーバ」として設定するか、156ページの「サーバ公開ルール」および121ページの「サイト共通ルール」を参照してルールを追加してください。

4. [次へ]をクリックする。

SIPサーバ公開の設定画面が表示され、SIPサーバの設定に進みます。



[戻る]をクリックすると、ファイル転送サーバ公開の設定画面に戻ります。

SIPサーバの設定

SIPサーバの設定では、外部ネットワークに公開するSIPサーバのIPアドレスを登録します。

1. 外部ネットワークへ公開するSIPサーバの有無を選択する。

   - 公開するSIPサーバはない
     公開するSIPサーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - 公開するSIPサーバはある
     公開するSIPサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

SIPサーバ公開の設定画面

2. 「公開IPアドレス」に公開するSIPサーバのIPアドレスを入力する。

SIPサーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。



ネットワークインタフェースの選択画面において、「アドレス変換(NAT/NAPT)を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。



かんたん設定ウィザードからは、外部に公開するSIPサーバとして1台までしか設定することができません。もし、2台以上のSIPサーバを設定するときには、「その他のサーバ」として設定するか、156ページの「サーバ公開ルール」および121ページの「サイト共通ルール」を参照してルールを追加してください。

かんたん設定

ファイアウォール > かんたん設定 [ヘルプ]

外部へ公開する「SIPサーバ」はありますか？

戻る 次へ

○ 公開するSIPサーバはない

◉ 公開するSIPサーバはある

サーバ	公開IPアドレス	→	内部IPアドレス
1台目	192.168.30.7	→	172.16.16.4

SIPサーバ公開の設定画面

4. [次へ]をクリックする。

その他の公開サーバの設定画面が表示され、その他のサーバ群の設定に進みます。



[戻る]をクリックすると、ネームサーバ公開の設定画面に戻ります。

外部ネットワークに公開するその他のサーバ群の設定

その他のサーバ群の設定では、外部ネットワークに公開するその他のサーバ群のIPアドレスやポート番号などを登録します。

1. これまで設定してきたウェブサーバ、メールサーバ、ファイル転送サーバ、ネームサーバ、SIPサーバ以外で外部ネットワークへ公開するサーバの有無を選択する。
   - その他の公開するサーバはない
     その他の公開するサーバがない場合は、このラジオボタンをクリックし、手順4に進みます。
   - その他の公開するサーバはある
     その他の公開するサーバがある場合は、このラジオボタンをクリックし、手順2に進みます。

その他の公開サーバの設定画面

2. 「公開IPアドレス」に公開するサーバのIPアドレスを入力し、右端のテキストボックスにポート番号を入力する。

サーバ公開の設定画面

3. ネットワークインタフェースの選択画面において、「アドレス変換（NAT/NAPT）を行う」のチェックボックスをチェックした場合は、「内部IPアドレス」に内部ネットワーク用のIPアドレスを入力する。

> **チェック**
>
> ネットワークインタフェースの選択画面において、「アドレス変換（NAT/NAPT）を行う」のチェックボックスにチェックしていなければ、「内部IPアドレス」は表示されません。

> **重要**
>
> **Express5800/SG300の外部インタフェースのIPアドレスを公開アドレスとして使用することもできますが、ポート番号がユーザ認証ウェブ（114ページ参照）と重複しないよう注意してください。**

サーバ公開の設定画面



かんたん設定ウィザードからは、外部に公開するその他のサーバ群として5台までしか設定することができません。もし、6台以上のサーバを設定するときには、156ページの「サーバ公開ルール」および121ページの「サイト共通ルール」を参照してルールを追加してください。

4. [次へ]をクリックする。

外部ネットワーク利用サービス選択の画面が表示され、外部ネットワークのサービスの利用の選択に進みます。



[戻る]をクリックすると、SIPサーバ公開の設定画面に戻ります。

外部サービスの利用の選択

内部ネットワークから利用する外部ネットワークのサービスを選択します。選択するサービスを以下に示します。

- ウェブサービス(HTTP/HTTPS)
- メールサービス(SMTP)
- ファイル転送サービス(FTP)
- ネームサービス(DNS)
- 時刻同期サービス(NTP)
- SIPサービス

1. サービスの利用の有無を選択する。



かんたん設定ウィザードからは、外部サービスとして上記に示す5つのサービスまでしか設定することができません。もし、これら以外のサービスを利用するときには、121ページの「サイト共通ルール」を参照してルールを追加してください。

かんたん設定

ファイアウォール > かんたん設定 [ヘルプ]

外部ネットワークに公開されている、どのようなサービスを利用しますか？

[戻る] [次へ]

■利用するサービス	
ウェブサービス(HTTP/HTTPS)	⦿利用する ○利用しない
メールサービス(SMTP)	⦿利用する ○利用しない
ファイル転送サービス(FTP)	⦿利用する ○利用しない
ネームサービス(DNS)	⦿利用する ○利用しない
時刻同期サービス(NTP)	⦿利用する ○利用しない
SIPサービス	⦿利用する ○利用しない

外部ネットワーク利用サービス選択の画面

2. [次へ]をクリックする。

より強固な不正アクセス対策の設定画面が表示され、不正アクセス対策レベルの設定に進みます。



[戻る]をクリックすると、その他のサーバ群の設定画面に戻ります。

不正アクセス対策レベルの設定

不正アクセス対策のレベルを設定します。対策のレベルには以下の3つがあります。

- ベーシック
- アドバンス
- 上記の対策を行わない

1. 不正アクセス対策レベルを選択する。



より強固な不正アクセス対策の設定画面

それぞれの対策について説明します。

[ベーシック]のラジオボタンを選択すると以下の不正アクセス対策を行います。

- Ping Sweep検知
  Ping Sweepとは、Pingを利用してネットワーク上で稼動するホストを調べることで、しばしば攻撃を仕掛ける前の事前調査として行われます。Ping Sweep検知では悪意を持った第三者によるPing Sweepを検知します。
- SYN Flood対策
  SYN Floodとは、攻撃対象のホストに対してSYNパケットを大量に送りつけるDoS攻撃の1つです。SYN Flood対策では悪意を持った第三者からSYN Flood攻撃を受けたとしても、サーバリソースの枯渇を防ぐことが可能です。
- traceroute対策
  ネットワークの経由情報からファイアウォールの所在を隠すことが可能です。
- IP Spoofing対策
  送信元情報を偽ったパケットを破棄することが可能です。

[アドバンス]のラジオボタンを選択すると、ベーシックレベルの対策に加えて、次の3つの不正アクセス対策を追加します。

- 通信流入量の制限
  Express5800/SG300では外部ネットワークからの過剰なアクセスを制限することが可能です。この機能では、外部ネットワークから受信するパケット量が上限値(70Mbps)を超えたとき、ファイアウォールを越えての新規の接続要求を拒絶します。これにより、DoS攻撃などの悪意を持った過負荷となる通信から内部サーバを保護します。

  パケット量は、宛先や送信元、ポートによらず、受信する全パケットの総量で測ります。パケット流入量の上限値や、制限を掛けるインタフェースの調整は詳細設定の流入量制限ルールから行うことができます。

- オートディフェンス
  ウェブサービス、メールサービスへの不正アクセスに対して応答を偽装することにより、正規サーバを不正アクセスから守ることが可能です。

  ウェブやメールのポートへ無作為にアクセスして応答するサーバを探し、不正アクセスを試みる不審者に対処する機能です。

  偽装応答に対して続けてアクセスしてきたときや、公開していないサーバのウェブやメールのポートに多数の接続(120秒に1000回以上)を要求してきたときは、不審者とみなして、その送信元からのすべてのアクセスを1時間禁止します。これにより、公開しているサーバへの攻撃を防ぐ可能性を高めます。

「上記の対策を行わない」のラジオボタンを選択すると、Express5800/SG300は上記のいずれの対策も行いません。

重要

- **オートディフェンス機能の対象ポートは、HTTP(ポート番号80)、SMTP(ポート番号25)です。独自のポート番号やHTTPS(ポート番号443)で公開しているサーバは対象外です。**
- **外部ネットワークから接続されるウェブサーバやメールサーバは、公開サーバとして必ず登録しておいてください。登録していないと、オートディフェンス機能により偽装応答が返ります。**
- **詳細設定のサイト共通ルール設定とサーバ公開ルール設定の各画面にあるウェブ専用フィルタのチェックボックスのチェックを外すとアドバンスレベルの不正アクセス対策の一部の機能が解除されます。逆に、不正アクセスのアドバンスレベルの選択を外すと、詳細設定のウェブ専用フィルタのいくつかのチェックボックスのチェックも外れます。**

ヒント

公開しているウェブサーバへの過剰アクセスを一時遮断する機能は、詳細設定のサーバ公開ルール画面のウェブ専用フィルタの設定から指定できます。

2. [次へ]をクリックする。

   ユーザ認証の利用選択画面が表示され、ユーザ認証の利用の有無の設定に進みます。

   ヒント

   [戻る]をクリックすると、外部ネットワーク利用サービス選択の画面に戻ります。

ユーザ認証の利用の設定

外部ネットワークから内部ネットワークに存在する端末にアクセスするときや、内部ネットワークから外部ネットワークに存在する端末にアクセスするときは、ファイアウォールとなるExpress5800/SG300を介して通信を行います。このとき、ユーザ認証によりユーザごとに使用する通信を許可することができます。ユーザ認証の利用の設定では、ユーザ認証を利用するかどうかを設定します。



リモートアクセスVPNを利用する場合は、「ユーザ認証を利用する」に設定してください。認証の受付は「すべてのネットワークから許可する」に設定してください。



ユーザの認証は、「ユーザ設定」で登録するユーザID、パスワードにより認証します。213ページの「ユーザ設定」を参照してください。
また、認証を行ったユーザごとに通信の許可を行う場合は、ユーザをユーザグループに所属させ、該当ユーザグループのグループルールを設定する必要があります。ユーザグループ設定とグループルール設定については、それぞれ231ページと141ページを参照してください。

1. ユーザ認証の利用の有無を選択する。

   - ユーザ認証を利用しない
     ユーザ認証を利用しない場合は、このラジオボタンをクリックし、手順4に進みます。
   - ユーザ認証を利用する
     ユーザ認証を利用する場合は、このラジオボタンをクリックし、手順2に進みます。

ユーザ認証の利用選択画面

2. ユーザ認証ウェブのポート番号を指定する。

   デフォルトでは「443」に設定されています。通常変更する必要はありません。

ユーザ認証の利用選択画面

3. ユーザ認証の受付を設定する。

- 内部ネットワークからのみ許可する
  ユーザ認証のためのアクセスを内部ネットワークからのみ受付けます。
- すべてのネットワークから許可する
  ユーザ認証のためのアクセスをどこからでも受付けます。

かんたん設定

ファイアウォール > かんたん設定　[ヘルプ]

ユーザ認証を利用しますか？

[戻る] [次へ]

○ ユーザ認証を利用しない

◉ ユーザ認証を利用する

ユーザ認証ウェブのポート番号を 443 とする
（分からない場合は、変更しないで下さい）

どこからの認証を許可しますか？
◉ 内部ネットワークからのみ許可する
○ すべてのネットワークから許可する

◉ 内部ネットワークからのみ許可する
○ すべてのネットワークから許可する

ユーザ認証の利用選択画面

4. [次へ]をクリックする。

設定内容確認画面が表示され、これまでの設定内容の確認に進みます。



- [戻る]をクリックすると、より強固な不正アクセス対策の設定画面に戻ります。
- ユーザ認証は詳細設定メニューの「認証設定」からも設定することができます。認証設定については、227ページを参照してください。

かんたん設定ウィザードでの設定内容の確認

かんたん設定ウィザードを利用して設定した内容を確認することができます。

1. 設定内容確認画面から以下の項目を確認する。



設定内容確認画面

- NAT/NAPTによるアドレス変換の設定の有無
  Express5800/SG300がアドレス変換を行うかどうか表示します。
  ブリッジ構成の場合は、「ブリッジ機能を利用する」と表示されます。
- 不正アクセス対策レベル
  不正アクセス対策レベルを表示します。
- ユーザ認証
  ユーザ認証を利用するかどうかを表示します。
- ネットワーク構成
  ネットワークの構成、外部ネットワークアドレス、内部ネットワークアドレス、DMZネットワークアドレスを図で表示します。
- 外部ネットワーク上の利用可能サービス
  内部ネットワークから利用できる外部ネットワーク上のサービスを一覧表示します。
- 外部ネットワークへ公開するサーバ
  外部ネットワークから利用できる内部ネットワーク上のサーバと、そのサーバの公開IPアドレス、内部IPアドレスを一覧表示します。

2. 設定した内容で問題なければ[設定]をクリックする。

   ルール適用画面が表示されます。



設定内容の適用に失敗すると、エラー内容が表示されます。その場合、再度設定をやり直してください。



[やり直し]をクリックすると、設定した内容は保持したままかんたん設定ウィザードのネットワーク構成の選択画面に戻り、最初から設定をやり直すことができます。

3. ［かんたん設定を終了］をクリックする。

ファイアウォールメニューに戻ります。

かんたん設定を終了

設定内容確認画面

詳細設定メニュー

かんたん設定ウィザードを利用して設定を行った後、細かい設定が必要な場合は、詳細設定メニューを使用します。



詳細設定を行うには、必ず一度はかんたん設定ウィザードでの設定を行う必要があります。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

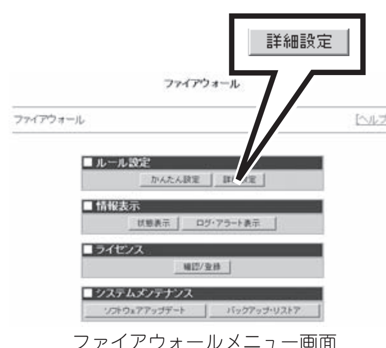
   詳細設定メニュー画面が表示されます。

   詳細設定メニューからは主に以下の内容を設定することができます。

   - ルール設定
     かんたん設定ウィザードで設定した内容をさらに詳しく設定することができます。
   - ユーザ設定
     ユーザ情報の登録、削除、更新といった管理やユーザ認証の設定を行います。
   - VPN設定
     VPNの詳細設定をすることができます。
   - ログ・アラート設定
     ログファイルやアラートファイルに関連する各種パラメータを設定することができます。

   重要

   「ルール設定」の中で、ボタンの下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。各項目の設定では、設定完了後、[登録]をクリックしますが、この段階では新しい設定内容を作成しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。



ファイアウォールメニュー画面



詳細設定メニュー画面

ルール設定

かんたん設定ウィザードで設定した内容をさらに詳しく設定することができます。
ルール設定では以下の項目を設定します。

サイト共通ルール .... 外部ネットワークと内部ネットワーク、あるいは外部ネットワークとDMZ、さらには内部ネットワークとDMZというように、Express5800/SG300を間に挟んだネットワークをサイトとして管理し、そのサイト内で常時適用されるルールを設定することができます。

グループルール .... サイト共通ルールでの設定に対して、グループ単位で例外的に許可するルールを設定することができます。

サーバ公開ルール .... 外部ネットワークにサーバを公開するための設定やアドレス変換(NAT)などを行うことができます。

流入量制限ルール .... DMZ/内部ネットワークに入ってくるパケット流量を制限することができます。

アドレスグループ .... アドレスごとにグループを作成することができます。サイト共通ルールやグループルールの発信元、宛先に指定することができます。

サービス .... サービスを新たに定義することができます。定義したサービスはサイト共通ルールやグループルールの通信種別に設定することができます。

ルール設定の履歴表示 .... 設定したルールの履歴を表示することができます。

インポート/エクスポート .... 各ルールの設定内容をエクスポートしたり、Express5800/SG300にインポートすることができます。



各ボタンの下に「編集中」と表示されている場合には、各種ルールを編集したままであることを示しています。[編集結果を適用]をクリックすれば、編集内容をExpress5800/SG300に適用することができます。
編集中のルールセットを破棄したい場合には、[最終更新状態に戻す]をクリックすれば、編集中のルールを破棄し、Express5800/SG300に適用した最終のルールセットの状態に戻すことができます。

設定作業の流れ

ここでは、かんたん設定ウィザードで設定をした後、詳細設定メニューを利用してさらに詳細な設定を行う場合の作業の流れを設定事例をもとに説明します。

■ 外部ネットワークから内部ネットワークやDMZ上のサーバへのアクセスを許可するには

1. サーバ公開ルールを設定する。
2. サイト共通ルールを設定する。
   このときNATを利用している場合、宛先は内部IPアドレスを指定します。
3. 詳細設定メニューで、サーバ公開ルールとサイト共通ルールの編集結果を適用する。

■ 内部ネットワークから外部ネットワークへのアクセスを許可するには

1. サイト共通ルールを設定する。
2. 詳細設定メニューで、サイト共通ルールの編集結果を適用する。

■ 認証されたユーザについてのアクセスを許可するには

1. グループ設定で、ユーザのグループを作成する。
2. ユーザ設定で、ユーザを作成してグループに所属させる。
3. グループルールを設定する。
4. 詳細設定メニューで、グループルールの編集結果を適用する。

■ 内部ネットワークユーザが閲覧する外部ネットワークのURLを制限するには

1. サイト共通ルールのウェブ専用フィルタの設定を行う。
2. サイト共通ルールで、「ウェブ専用フィルタを経由して見る」を有効にする。
3. 詳細設定メニューで、サイト共通ルールの編集結果を適用する。

サイト共通ルール

サイト共通ルールとは、Express5800/SG300を導入した環境において、外部ネットワークと内部ネットワーク、あるいは外部ネットワークとDMZ、さらには内部ネットワークとDMZというように、Express5800/SG300を間に挟んだネットワーク内で常時適用されるルールのことです。
サイト共通ルールでは、以下のような設定・管理を行うことができます。

- サイト共通ルールの設定内容の確認
- サイト共通ルールの追加
- サイト共通ルールの削除
- サイト共通ルールの更新
- ルール評価順の入れ替え
- 内部から外部への通信におけるウェブ専用フィルタの設定

サイト共通ルールの設定内容の確認

かんたん設定ウィザードから設定したサイト共通ルールや、すでに設定したルールはサイト共通一覧画面から確認することができます。

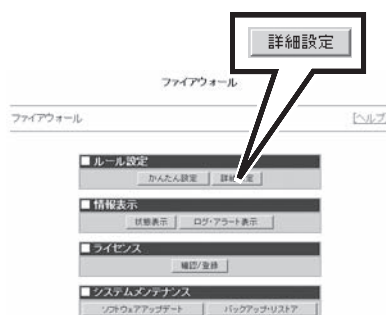
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

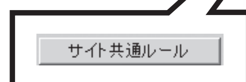
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

ルール設定一覧画面が表示されます。表示される内容は以下の通りです。





詳細設定メニュー画面

項　目	説　明	
No.	ルールの番号です。通信を通すか否かの判定の際は、番号の若いルールから順番に評価した結果、最初にマッチしたルールに基づいて処理されます。	
発信元	パケットの発信元を表すIPアドレス、ネットワークアドレス、あるいは内部、外部、DMZのいずれかです。	
宛先	パケットの宛先を表すIPアドレス、ネットワークアドレス、あるいは内部、外部、DMZのいずれかです。	
通信種別	パケットのプロトコル種別を表します。	
処理		パケットを通します。
		パケットを破棄し、発信元へ応答を返しません。
		パケットを拒否し、発信元へエラーを返します。
記録		通信のログを残します。
		通信のログを残すとともにアラート情報も残します。
	［空白］	ログもアラートも残しません。
コメント		コメントが設定されています。クリックすると、別ウィンドウでコメントの内容を表示します。
	［空白］	コメントは設定されていません。



サイト共通ルール設定画面

ヒント

- 画面右上の「設定履歴」をクリックすると、「かんたん設定」と「ルール設定」での設定内容の履歴が表示されます。
- 画面右上の「かんたん設定(ネットワーク構成)の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。
- 発信先、宛先、通信種別のリンクをクリックすると、定義されたアドレスグループ、またはサービスの内容を確認できます。

具体的なサイト共通ルール一覧の事例を示します。

No.	発信元		宛先		通信種別	処理	記録	コメント
1	内部		内部		任意			
□ 2	外部			192.168.30.20	tcpすべて			
□ 3	部門ネット1 部門ネット2		ウェブサーバ		http https			

ルール設定一覧

ルールの1行目: 内部ネットワークにある端末間のすべての通信を許可することを表します。

ルールの2行目: 外部ネットワークから192.168.30.20のIPアドレスを持つ端末へのTCP通信をすべて拒否し、その通信ログとアラート情報を残すことを表します。コメントをクリックすると、設定されているコメントの内容を確認できます。

ルールの3行目: 部門ネット1、部門ネット2からウェブサーバへのHTTP通信、HTTPS通信を許可しログを残すことを表します。コメントをクリックすると、設定されているコメントの内容を確認できます。

サイト共通ルールの追加

必要に応じてサイト共通ルールを追加することができます。

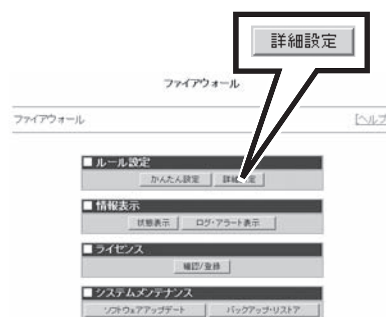
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

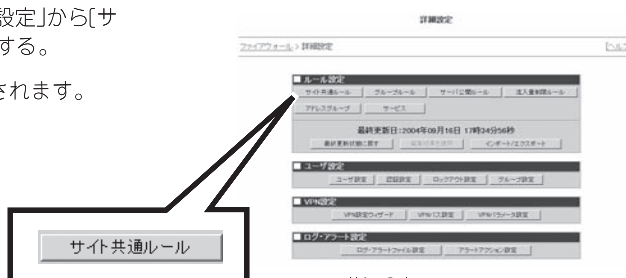
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

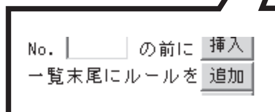
   ルール設定一覧画面が表示されます。



詳細設定メニュー画面

4. 表の途中に挿入する場合は、「No.の前に『挿入』」の「No.」のテキストボックスにルールの番号を入力し、「No.の前に『挿入』」をクリックする。表の末尾に追加する場合は、「一覧末尾にルールを『追加』」をクリックする。

ルール設定追加画面が表示されます。



サイト共通ルール設定画面

チェック

「No.」のテキストボックスに値を入れずに「No.の前に『挿入』」をクリックすると、エラー内容を示す画面を表示します

ヒント

「かんたん設定ウィザード」で設定されたルール(背景ピンク色)の間にも新しくルールを挿入することはできますが、再度「かんたん設定ウィザード」を用いてルールを再生成した場合、追加したルールは一覧の上部に表示され、「かんたん設定ウィザード」で設定したルールよりも評価順が上位になります。

5. ルール設定追加画面に表示される各項目を設定する。

ルール設定追加画面

項目		説明
処理	許可	パケットを通します。
	破棄	パケットを破棄し、発信元へ応答を返しません。
	拒否	パケットを拒否し、発信元へエラーを返します。
発信元	ユーザ指定	ユーザの指定した発信元に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、180ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークからの通信です。
	内部	内部ネットワークからの通信です。
	DMZ	DMZからの通信です。
	任意	発信元に関わらず処理を適用します。
	上記指定以外	チェックボックスをチェックすると、選択した発信元以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を発信元とする通信に対し処理を適用します。
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、180ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。
	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイア ウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが表示されます。サービスのリストには、191ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。
コメント		任意のコメントを入力できます。最大で1000文字までを受け付けますが、右大不等号（<）および左大不等号（>）を含めることはできません。



- 発信元および宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。

6. ［登録］をクリックする。

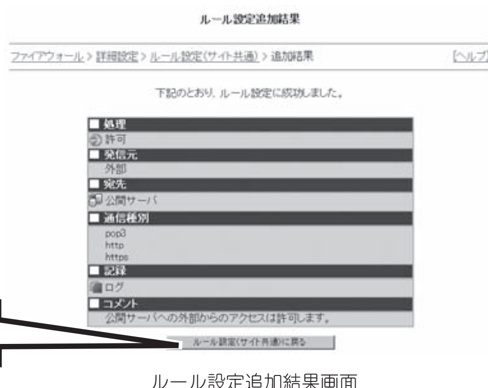
ルール設定追加結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

7. ［ルール設定（サイト共通）に戻る］をクリックする。

追加したルールが反映されたルール設定一覧画面が表示されます。



ルール設定追加結果画面

8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。



詳細設定メニュー

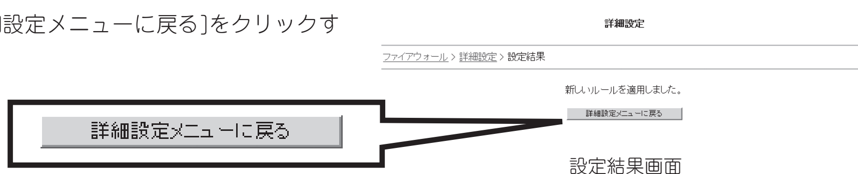


- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。



設定結果画面

サイト共通ルールの削除

不要になったサイト共通ルールを削除することができます。

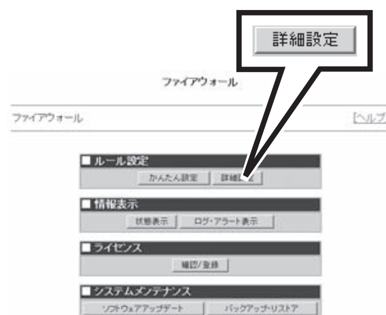
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

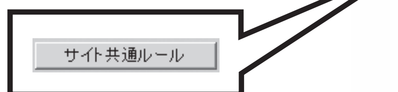
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

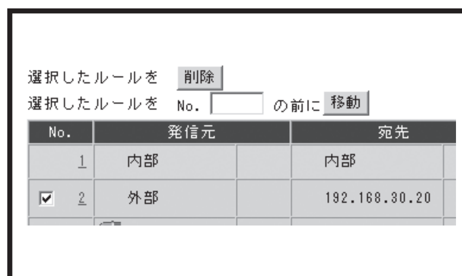
   ルール設定一覧画面が表示されます。





詳細設定メニュー画面

4. 削除したいルールの「No.」の横に表示されるチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。





サイト共通ルール設定一覧画面



- 一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、サイト共通ルールの設定から削除することはできません。
- 「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。

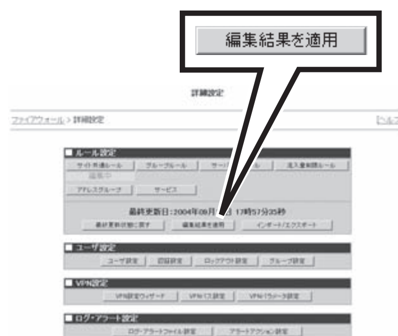
5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

   サイト共通ルールが削除され、削除確認の別ウィンドウが閉じます。



[キャンセル]をクリックすると、削除されずにルール設定一覧画面に戻ります。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

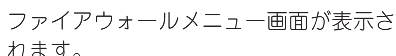
8. [詳細設定メニューに戻る]をクリックする。



サイト共通ルールの更新

一度設定したサイト共通ルールの内容を変更することができます。

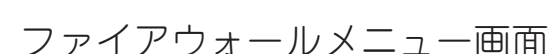
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。



   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

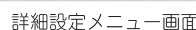
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

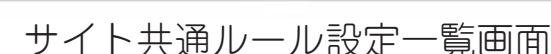
   ルール設定一覧画面が表示されます。



詳細設定メニュー画面

4. 変更したいルールの「No.」をクリックする。

   ルール設定更新画面が表示されます。



サイト共通ルール設定一覧画面



一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、「記録」および「コメント」のみ変更することができます。その他の項目を更新する場合は、もう一度「かんたん設定ウィザード」に戻って設定をやり直してください。



「かんたん設定ウィザード」を用いてルールを再生成すると、「かんたん設定ウィザード」を経由して設定されたルールの「記録」および「コメント」の項目がデフォルト値(「記録」は[記録しない]、「コメント」は空欄)に戻ります。

通信ログを記録する必要がある場合やコメントを登録する場合は、「かんたん設定ウィザード」からではなく、詳細設定メニューの「ルール設定」よりルールを設定することを推奨します。

5. ルール設定更新画面に表示される各項目を設定する。

ルール設定更新画面

項　目		説　明
処理	許可	パケットを通します。
	破棄	パケットを破棄し、発信元へ応答を返しません。
	拒否	パケットを拒否し、発信元へエラーを返します。
発信元	ユーザ指定	ユーザの指定した発信元に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、180ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークからの通信です。
	内部	内部ネットワークからの通信です。
	DMZ	DMZからの通信です。
	任意	発信元に関わらず処理を適用します。
	上記指定以外	チェックボックスをチェックすると、選択した発信元以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を発信元とする通信に対し処理を適用します。

項　目		説　明
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。 テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループは、180ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。
宛先	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイア ウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが表示されます。サービスのリストには、191ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。
コメント		任意のコメントを入力できます。最大で1000文字までを受け付けますが、右大不等号（<）および左大不等号（>）を含めることはできません。



- 発信元および宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。

6. [登録]をクリックする。

ルール設定更新結果画面が表示されます。



登録に失敗した場合は、エラー内容を示す画面を表示します。

7. ［ルール設定（サイト共通）に戻る］をクリックする。

   更新したルールが反映されたルール設定一覧画面が表示されます。



ルール設定更新結果画面

8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

   更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. ［詳細設定メニューに戻る］をクリックする。



ルール評価順の入れ替え

サイト共通ルールの評価順を入れ替えることができます。

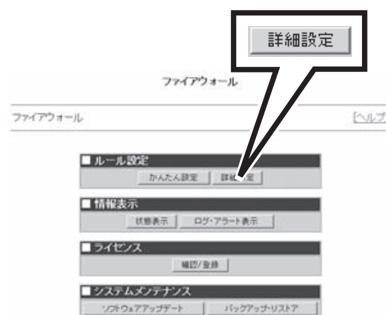
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

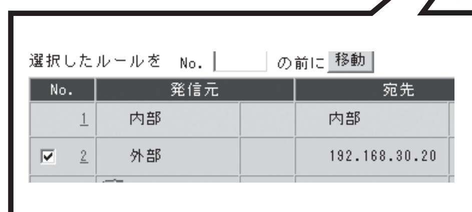
3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   サイト共通ルール一覧画面が表示されます。



詳細設定メニュー画面

4. 評価順を入れ替えたいルールの「No.」の横に表示されるチェックボックスをチェックし、さらに「選択したルールをNo.の前に『移動』」の「No.」のテキストボックスにルールの番号を入力し、「選択したルールをNo.の前に『移動』」クリックする。





サイト共通ルール設定一覧画面



- 「かんたん設定ウィザード」で設定されたルール(背景ピンク色)の間にもルールを移動することはできますが、再度「かんたん設定ウィザード」を用いてルールを再生成した場合、移動したルールは一覧の上部に表示され、「かんたん設定ウィザード」で設定したルールよりも評価順が上位になります。
- 「かんたん設定ウィザード」で設定されたルールよりも下位にあるルールについては、再度「かんたん設定ウィザード」を用いてルールを再生成した場合でも、評価順は下位のままです。

評価順が反映されたルール設定一覧画面が表示されます。

5. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順4で「選択したルールをNo.の前に『移動』」をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの評価順変更前の状態に戻ります。**

6. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しい評価順のサイト共通ルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

7. [詳細設定メニューに戻る]をクリックする。



内部から外部への通信におけるウェブ専用フィルタの設定

内部ネットワークまたはDMZから外部ネットワークへのHTTP通信のフィルタリング設定を行うことができます。ここでは、アクセス制御するURLを設定することで内部ネットワークから外部ネットワークへのHTTP通信を制限します。

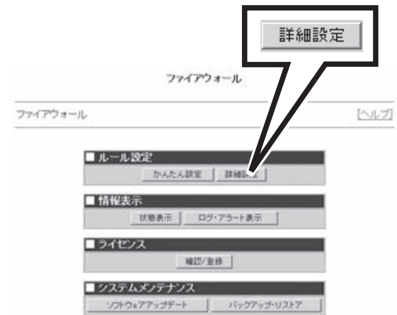
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   ルール設定一覧画面が表示されます。



詳細設定メニュー画面

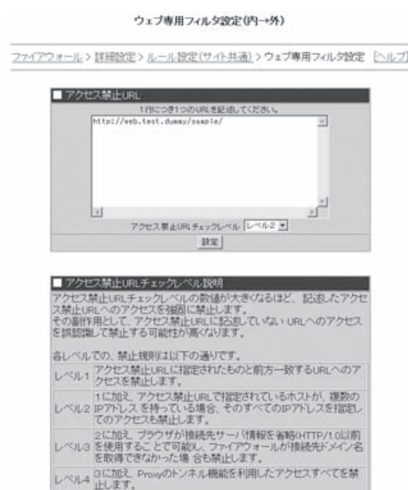
4. 「オプション」の「ウェブ専用フィルタ設定」をクリックする。

   ウェブ専用フィルタ設定(内→外)画面が表示されます。



サイト共通ルール設定一覧画面

5. 「アクセス禁止URL」のテキストエリアにHTTP通信を拒否したいURLを入力する。



ウェブ専用フィルタ設定(内→外)画面



- 1行につき1つのURLを指定してください。URLとして最大で1000バイトまでの文字列を指定できます。
- URLの記述は、「http://」から始め、パス部分まで設定することができます。
  ただし、パスごとに設定する必要はなく、指定した文字列で始まるURLはすべてアクセス制御がかかります。たとえば、「http://web.server.name/data1/」と指定すると、「http://web.server.name/data1/data2/」などもアクセス禁止になります。
- URLの一部として、「＊」が利用できます。たとえば「web*.server.name」というように指定することもできます。



この機能の対象ポートは、HTTP(ポート番号80)です。独自のポート番号で公開していたり、セキュリティで保護されている(https)ウェブサーバには使用できません。

6. アクセス禁止URLチェックレベルをプルダウンメニューより選択する。

   アクセス禁止レベルは数値が大きくなるほど、設定したURLへのアクセス制御を強固にします。アクセスレベルの詳細については、画面に表示される内容を確認してください。

7. ［設定］をクリックする。

   ウェブ専用フィルタ設定（内→外）結果画面が表示されます。

ウェブ専用フィルタ設定（内→外）画面

8. ［ルール設定（サイト共通）に戻る］をクリックする。

   サイト共通ルール一覧画面が表示されます。

ウェブ専用フィルタ設定（内→外）結果画面

9. 「内部からウェブ専用フィルタ経由で外部のウェブサイトを見る。」のチェックボックスにチェックし、［確定］をクリックする。

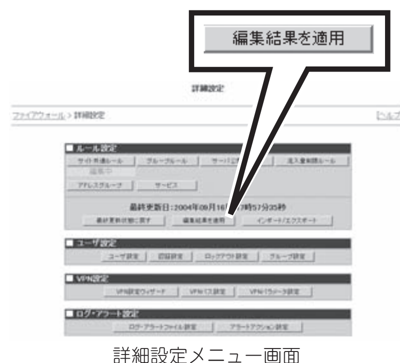
   設定結果画面が表示されるので、［ルール設定（サイト共通）に戻る］をクリックします。

サイト共通ルール設定一覧画面

重要

[確定]をクリックしないと、ウェブ専用フィルタ設定をしてもフィルタリング機能は有効になりません。逆にウェブ専用フィルタ設定をしないでフィルタリング機能を有効にしても効果はありません。

10. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順9で[確定]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はフィルタリング機能の設定前の状態に戻ります。**

11. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

フィルタリング設定がExpress5800/SG300に適用され、設定結果画面が表示されます。

12. [詳細設定メニューに戻る]をクリックする。



グループルール

グループルールとは、グループに所属するユーザが認証を行うことで適用されるルールのことです。ここでは、サイト共通ルールでの設定に対し、グループ単位で例外的に許可するルールを設定します。たとえば、以下のような設定ができます。

- サイト共通ルールではHTTP通信を拒否するが、ある部署に所属するメンバだけには、指定する端末へのHTTP通信を許可する
- サイト共通ルールではサーバへのアクセスを拒否するが、プロジェクトメンバに対してだけは、プロジェクトで利用するサーバへのアクセスを許可する

Express5800/SG300は、ユーザの所属しているグループのルールに従って通信の種別や宛先から通信の許可、アクセスログの取得などの処理を判断します。ユーザが所属するグループルールにおいては上位に表示されるものから順番に評価を行います。



ユーザ認証実行後、有効時間内は所属しているグループルールが適用されます。有効時間内を過ぎてから、ユーザがグループルールで許可されたExpress5800/SG300を超える通信を行う場合は、再度ログインする必要があります。

グループルールでは、以下のような設定・管理を行うことができます。

- グループルールの設定内容の確認
- グループルールの追加
- グループルールの削除
- グループルールの更新



あらかじめグループの設定を行っていないとグループルールの設定・管理を行うことはできません。グループの設定については、231ページの「グループ設定」を参照してください。

グループルールの設定内容の確認

すでに設定したルールはグループルール一覧画面から確認することができます。

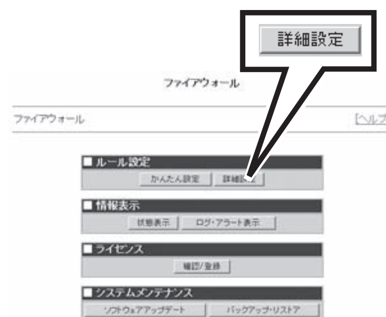
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

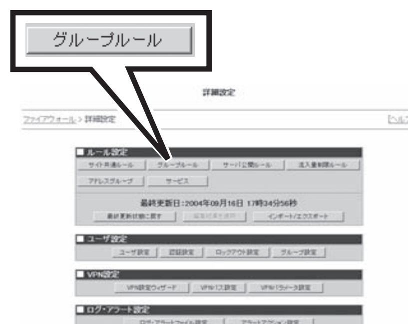
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

   グループルール一覧画面が表示されます。表示される内容は以下の通りです。



詳細設定メニュー画面

項　目	説　明
グループ番号	[001]のような形式でシステムがグループに付与した番号が表示されます。
グループ名	グループ名です。
認証有効時間	ユーザ認証後グループルールが適用される有効時間です。
トランスポートVPNパス	VPNパスを使用するかどうかを表示します。
No.	ルールの番号です。通信を通すか否かの判定の際は、番号の若いルールから順番に評価した結果、最初にマッチしたルールに基づいて処理されます。
発信元	「ユーザが使用中のホスト」です。
宛先	パケットの宛先を表すIPアドレス、ネットワークアドレス、あるいは内部、外部、DMZ、任意、ファイアウォール自身、指定した宛先以外のいずれかです。

項　目	説　明	
通信種別	パケットのプロトコル種別を表します。	
処理		パケットを通します。
記録		通信のログを残します。
		通信のログを残すとともにアラート情報も残します。
	［空白］	ログもアラートも残しません。
コメント		コメントが設定されています。クリックすると、別ウィンドウでコメントの内容を表示します。
	［空白］	コメントは設定されていません。



グループルール一覧画面



画面右上の「かんたん設定（ネットワーク構成）の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。

上記の画面を例にして具体的なグループルール一覧の事例を示します。

[002]のグループルールでは、group2に所属するユーザはExpress5800/SG300上での認証に成功すると、以下のルールが適用されます。認証の有効時間は60分です。

ルールの1行目:　ユーザの端末と内部ネットワークにある端末間のすべての通信を許可することを表します。コメントをクリックすると、設定されているコメントの内容を確認できます。

ルールの2行目:　ユーザの端末から外部ネットワークへのHTTP通信、HTTPS通信を許可することを表します。コメントをクリックすると、設定されているコメントの内容を確認できます。

グループルールの追加

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

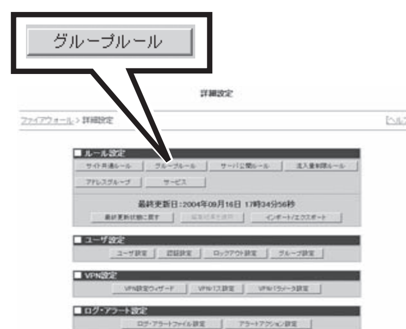
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

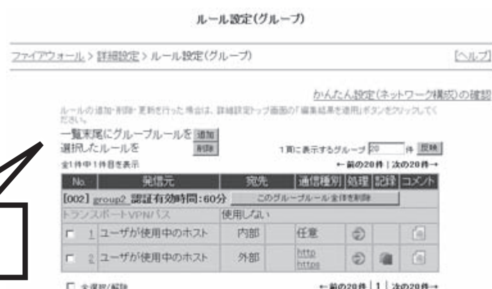
   グループルール一覧画面が表示されます。

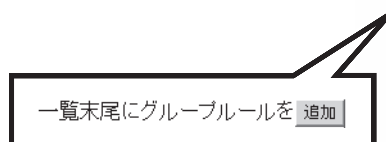


詳細設定メニュー画面

4. 「一覧末尾にグループルールを『追加』」をクリックする。

   グループ選択画面が表示されます。





グループルール一覧画面

5. ルールを追加するグループ名のラジオボタンをクリックし、「選択したグループのグループルールを『追加』」をクリックする。

選択したグループのルール一覧画面が表示されます。

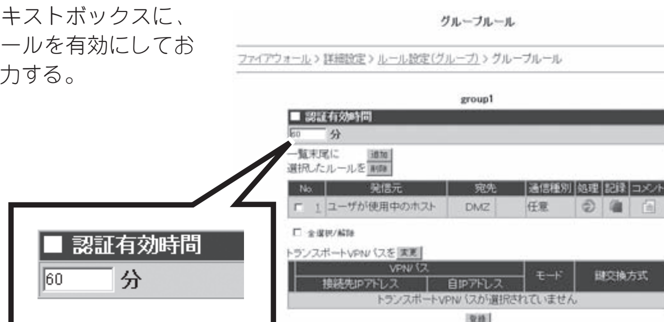


グループ選択画面



グループルールの一覧画面からグループ名をクリックすることでも、選択したグループのルール一覧画面を表示することができます。

6. 「認証有効時間」のテキストボックスに、ユーザ認証の後、ルールを有効にしておく時間を分単位で入力する。



選択したグループのルール一覧画面

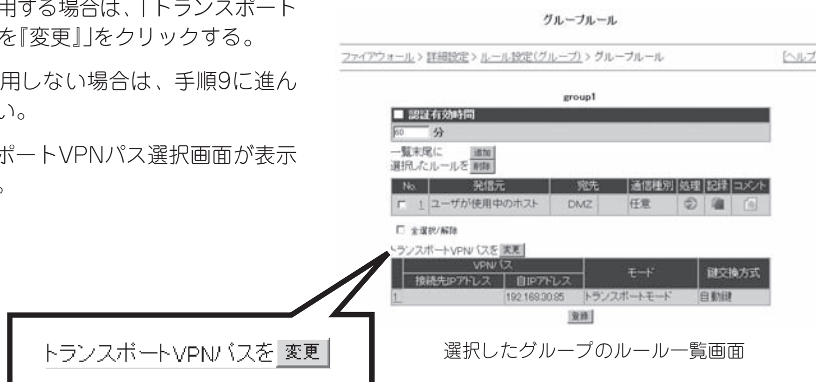


設定した有効期限を過ぎてから、ユーザがグループルールで許可されたExpress5800/SG300を超える通信を行う場合は、再度ログインする必要があります。

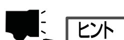
7. ある特定のアドレスから通信を行う際にVPNを利用する場合は、「トランスポートVPNパスを『変更』」をクリックする。

VPNを利用しない場合は、手順9に進んでください。

トランスポートVPNパス選択画面が表示されます。



選択したグループのルール一覧画面



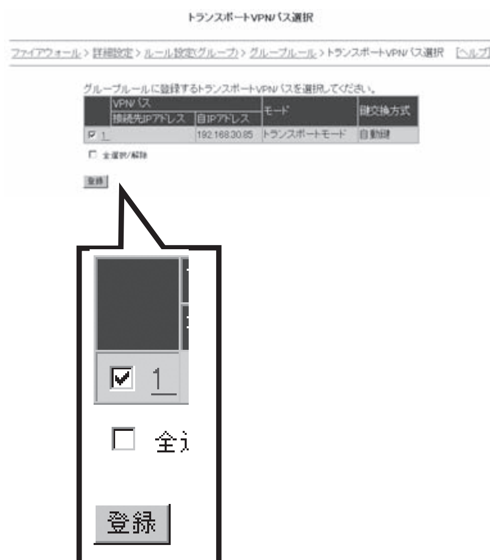
トランスポートVPNパスはあらかじめVPNパスを設定していないと表示されません。トランスポートVPNパスの設定については、240ページの「VPN設定」を参照してください。

8. 表示されるトランスポートVPNパスの中から利用するVPNパスのチェックボックスをチェックし、［登録］をクリックする。

選択したグループルールの一覧画面に戻ります。引き続き、グループルールの設定を行う場合は、手順9に進みます。ここでグループルールの設定を終了する場合は、手順13に進みます。



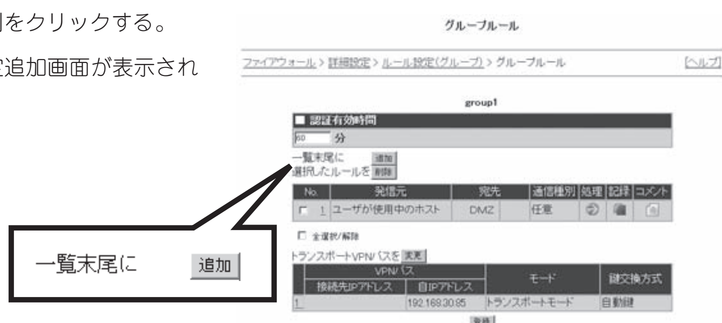
選択したグループのルール一覧画面で、追加したVPNパスの番号をクリックすると、そのVPNパスの詳細設定を確認することができます。



トランスポートVPNパス選択画面

9. 「一覧末尾に『追加』」をクリックする。

グループルール設定追加画面が表示されます。



選択したグループのルール一覧画面

10. グループルール設定追加画面に表示される各項目を設定する。

項　目		説　明
処理	許可	パケットを通します。設定の変更はできません。
発信元	ユーザが使用中のホスト	ユーザが使用している端末を発信元とする通信にルールを適用します。設定の変更はできません。
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、［←］をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループのリストには、180ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。
	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイアウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。

項　目		説　明
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが挿入されます。サービスのリストには、191ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。
コメント		任意のコメントを入力できます。最大で1000文字までを受け付けますが、右大不等号（<）および左大不等号（>）を含めることはできません。



- 宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。



グループルール設定追加画面

11. [登録]をクリックする。

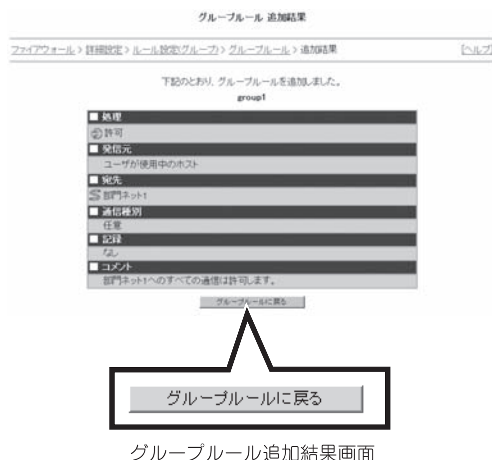
グループルール追加結果画面が表示されます。



グループルールの登録に失敗した場合は、エラー内容を示す画面が表示されます。

12. ［グループルールに戻る］をクリックする。

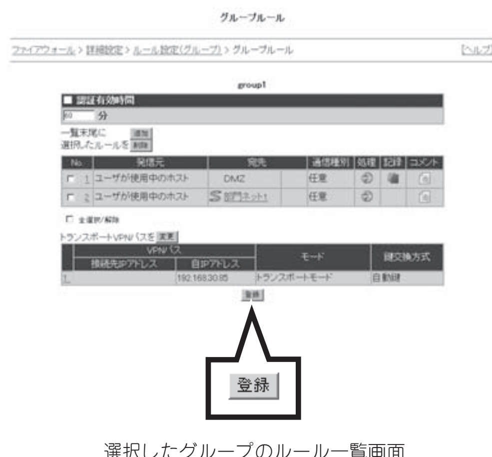
追加したルールが反映された、選択したグループのルール一覧画面が表示されます。



グループルール追加結果画面

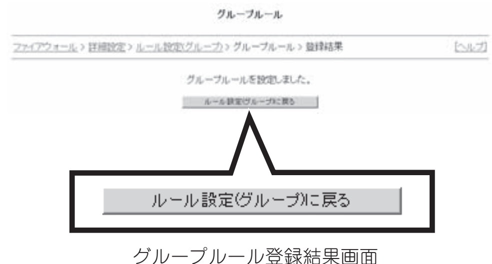
13. ［登録］をクリックする。

グループルール登録結果画面が表示されます。



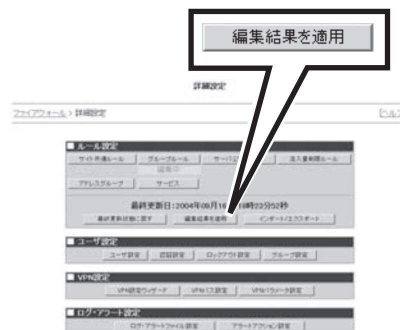
選択したグループのルール一覧画面

14. ［ルール設定（グループ）に戻る］をクリックする。



グループルール登録結果画面

15. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。



詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順11で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。

16. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

17. ［詳細設定メニューに戻る］をクリックする。



グループルールの削除

設定したグループルールを削除することができます。

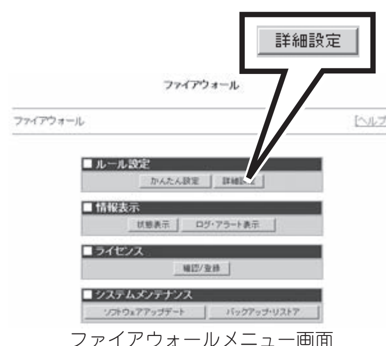
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

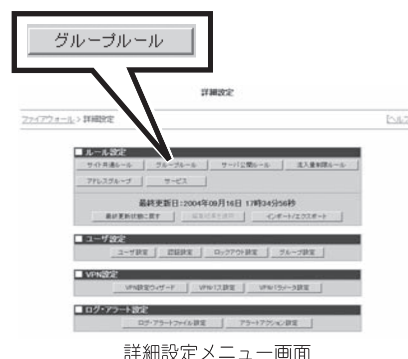
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

   グループルール一覧画面が表示されます。



詳細設定メニュー画面

4. 削除したいルールの「No.」の横に表示されているチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。





グループルール一覧画面



- 「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。
- グループルール一覧からグループ名をクリックし、選択したグループのルール一覧画面からルールを削除することもできます。
- [このグループルール全体を削除]をクリックすると、選択したグループのグループルールがすべて削除されます。

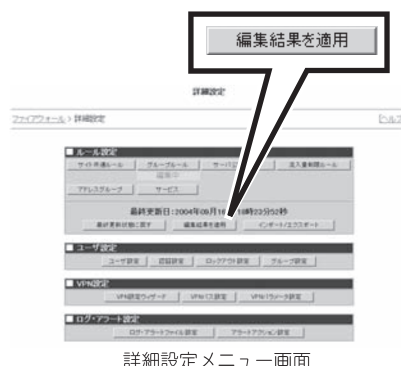
5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。

   グループルールが削除され、ルールが削除されたグループルール一覧画面が表示されます。



[キャンセル]をクリックすると、削除されずにグループルール一覧画面に戻ります。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。

詳細設定

ファイアウォール > 詳細設定 > 設定結果

新しいルールを適用しました。



グループルールの更新

一度設定したグループルールの内容を変更することができます。

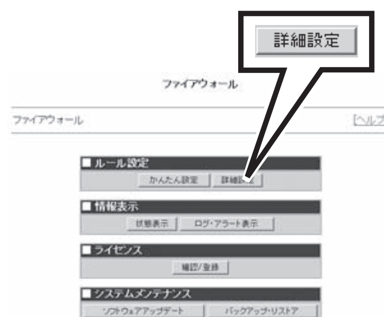
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

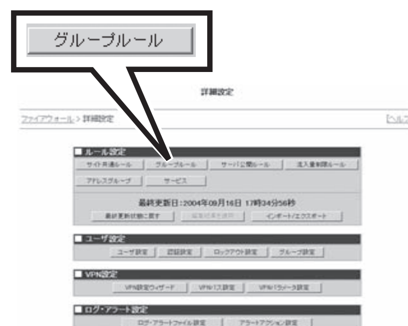
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[グループルール]をクリックする。

   グループルール一覧画面が表示されます。

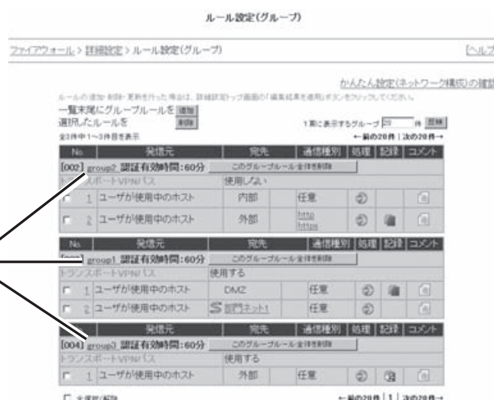


詳細設定メニュー画面

4. グループ名をクリックする。

   選択したグループのルール一覧画面が表示されます。

グループ名



グループルール一覧画面

5. 変更したいルールの「No.」をクリックする。

グループルール設定更新画面が表示されます。





選択したグループのルール一覧画面

6. グループルール設定更新画面に表示される各項目を設定する。

項　目		説　明
処理	許可	パケットを通します。設定の変更はできません。
発信元	ユーザが使用中のホスト	ユーザが使用している端末を発信元とする通信にルールを適用します。設定の変更はできません。
宛先	ユーザ指定	ユーザの指定した宛先に対し処理を適用します。テキストエリアにアドレスを直接入力するか、アドレスグループをリストから指定します。アドレスグループから指定する場合は、アドレスグループのリストからアドレスグループを選択し、[←]をクリックします。クリックするとテキストエリアに選択したアドレスグループが挿入されます。アドレスグループのリストには、180ページの「アドレスグループ」で登録したものが表示されます。
	外部	外部ネットワークへの通信です。
	内部	内部ネットワークへの通信です。
	DMZ	DMZへの通信です。
	任意	宛先に関わらず処理を適用します。
	ファイアウォール自身	ファイアウォール自身への通信です。
	上記指定以外	チェックボックスをチェックすると、選択した宛先以外の通信に対し処理を適用します。たとえば、「DMZ」を選択し「上記指定以外」をチェックすればDMZ以外を宛先とする通信に対し処理を適用します。
通信種別	ユーザ指定	ユーザの指定したプロトコル種別に対して処理を適用します。テキストエリアにプロトコル種別を直接入力するかサービス種別をリストから指定します。サービス種別から指定する場合は、サービスのリストからサービス種別を選択し、[←]をクリックします。クリックするとテキストエリアに選択したサービスが挿入されます。サービスのリストには、191ページの「サービス」で登録したものと標準定義サービスが表示されます。
	任意	通信種別に関わらず処理を適用します。
記録	なし	ログもアラートも残しません。
	ログ	通信のログを残します。
	アラート	通信のログを残すとともにアラート情報も残します。
コメント		任意のコメントを入力できます。最大で1000文字までを受け付けますが、右大不等号（<）および左大不等号（>）を含めることはできません。



- 宛先が含むアドレスグループのメンバの数の合計は、直接入力したアドレスの数を含めて最大50個までです。
- 通信種別が含むサービスのメンバの数の合計は、直接入力した要素の数を含めて最大50個までです。

7. ［登録］をクリックする。

   グループルール更新結果画面が表示されます。



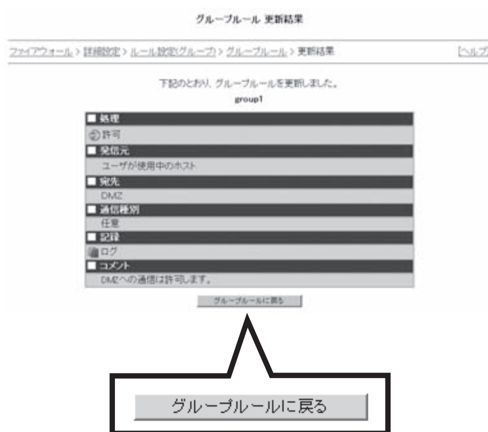
グループルールの更新に失敗した場合はエラー内容を示す画面が表示されます。



グループルール設定更新画面

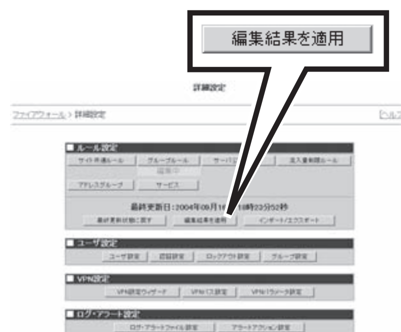
8. ［グループルールに戻る］をクリックする。

   更新したルールが反映された選択したグループのルール一覧画面が表示されます。



グループルール更新結果画面

9. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順7で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。

10. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

11. [詳細設定メニューに戻る]をクリックする。



ファイアウォール機能の設定方法

サーバ公開ルール

サーバ公開ルールとは、Express5800/SG300を導入した環境において、DMZまたは、内部ネットワーク上にあるサーバを外部ネットワークに公開する際に、アドレス変換(NAT)およびウェブ/メール専用フィルタの制御を行うためのルールのことです。
サーバ公開ルールでは、以下のような設定・管理を行うことができます。

- サーバ公開ルールの設定内容の確認
- サーバ公開ルールの追加
- サーバ公開ルールの削除
- サーバ公開ルールの更新
- 外部から内部への通信におけるウェブ専用フィルタの設定

サーバ公開ルールの設定内容の確認

かんたん設定ウィザードから設定したサーバ公開ルールや、すでに設定したルールはサーバ公開ルール一覧画面から確認することができます。

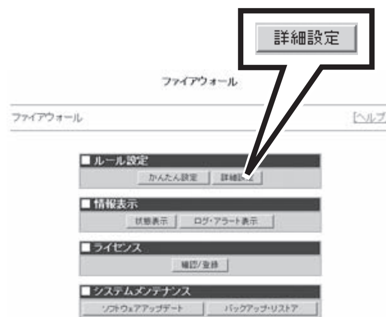
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



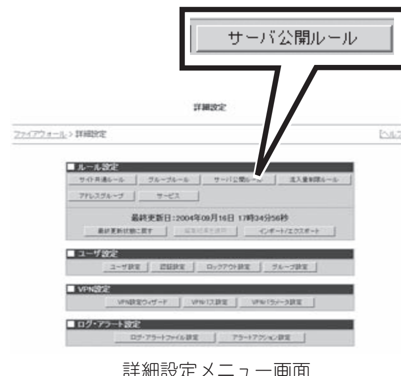
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から［サーバ公開ルール］をクリックする。



詳細設定メニュー画面

サーバ公開ルール一覧画面が表示されます。表示される内容は以下の通りです。

項　目	説　明	
公開IPアドレス	外部ネットワークへ公開するサーバのIPアドレスです。	
ポート	外部ネットワークへ公開するサーバのポート番号です。	
内部IPアドレス	内部ネットワークでのサーバのIPアドレスです。	
ポート	内部ネットワークでのサーバのポート番号です。	
記録	（アイコン）	通信のログを残します。
	［空白］	ログもアラートも残しません。
コメント	（アイコン）	コメントが設定されています。クリックすると、別ウィンドウでコメントの内容を表示します。
	［空白］	コメントは設定されていません。


サーバ公開ルール一覧画面



- 画面右上の「かんたん設定（ネットワーク構成）の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。
- 内部ネットワーク上の端末のアドレスをすべて本ファイアウォールのアドレスで置き換える機能(NAPT)は、かんたん設定のインタフェースの選択画面から設定します。



- この画面でサーバ公開の設定をしても、アクセス許可はされません。サーバへのアクセス許可についてはサイト共通ルール画面からルールを設定する必要があります。サイト共通ルール設定の際は、公開IPアドレスではなく、内部IPアドレスで設定してください。
- Express5800/SG300の外部インタフェースのIPアドレスを公開アドレスとして使用することもできますが、公開するポート番号がユーザ認証ウェブ(114ページ参照)と重複しないよう注意してください。
- ウェブ専用フィルタ設定、不正アクセス対策(アドバンスレベル)設定は、サーバ公開ルールに従ってアクセス制限を行います。

  外部ネットワークからアクセスするウェブサーバやメールサーバは、すべて登録してください。

具体的なサーバ公開ルール一覧の事例を示します。

No.	公開IPアドレス	ポート	内部IPアドレス	ポート	記録	コメント
1	192.168.30.30	tcp/80	192.168.1.30	80		
2	192.168.30.31	tcp/443	192.168.1.31	443		
3	192.168.30.32	tcp/25	192.168.1.32	25		
4	192.168.30.33	tcp/21	192.168.1.33	21		
5	192.168.30.36	udp/5060	192.168.1.36	5060		
☐ 6	192.168.30.185	tcp/80	192.168.20.161	80		
☑ 7	192.168.30.40	全部	192.168.10.5	全部		

サーバ公開ルール一覧画面

ルールの2行目: 内部アドレス192.168.1.31の端末がTCPポート443番で待ち受けているサービスを、外部ネットワークへはIPアドレス192.168.30.31、TCPポート443番で公開することを示しています。

ルールの3行目: 内部アドレス192.168.1.32の端末がTCPポート25番で待ち受けているサービスを、外部ネットワークへはIPアドレス192.168.30.32、TCPポート25番で公開することを示しています。

ルールの6行目: 内部アドレス192.168.20.161の端末がTCPポート80番で待ち受けているサービスを、外部ネットワークへはIPアドレス192.168.30.185、TCPポート80番で公開することを示しています。

ルールの7行目: 内部アドレス192.168.10.5の端末が待ち受けているサービスを、外部ネットワークへはIPアドレス192.168.30.40で公開することを示しています。コメントをクリックすると、設定されているコメントの内容を確認できます。

サーバ公開ルールの追加

必要に応じてサーバ公開ルールを追加することができます。

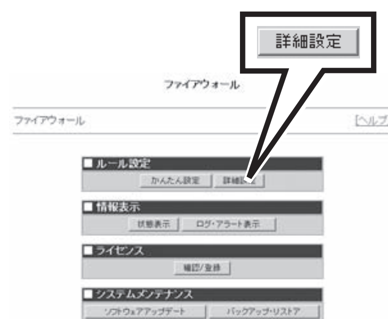
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

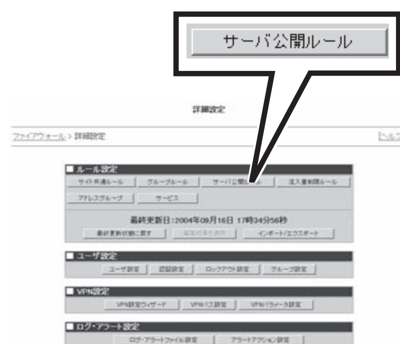
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。



詳細設定メニュー画面

4. 「一覧末尾にルールを『追加』」をクリックする。

   ルール設定追加画面が表示されます。



サーバ公開ルール一覧画面

5. ルール設定追加画面に表示される各項目を入力する。

ルール設定追加画面

項　目	説　明
外部公開IPアドレス	外部ネットワークへ公開するIPアドレスを入力します。
内部IPアドレス	サーバの実際のIPアドレスを指定します。「外部公開IPアドレス」と異なる場合は、そのIPアドレスを入力します。「外部公開IPアドレス」と同じ場合は、「アドレス変換しない」をクリックします。
ポート	ポート番号の指定を行うかどうかを選択します。特定のポート番号についてのみ公開するか、ポート番号の変換を行う場合には、外部ネットワークへ公開するポート番号と、対応する内部ネットワークのポート番号を入力します。
記録	作成するルールに該当する通信パケットを検出したとき、ログ情報としてのみファイルに出力するか、それともファイルにはいっさい記録しないかを設定します。
コメント	任意のコメントを入力できます。最大で1000文字までを受け付けますが、右大不等号（<）および左大不等号（>）を含めることはできません。

6. ［登録］をクリックする。

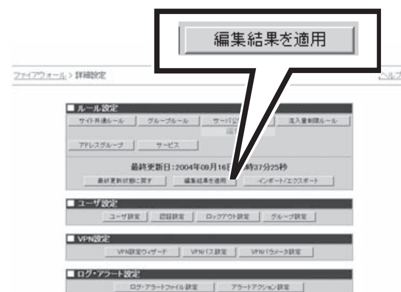
ルール設定追加結果画面が表示されます。

7. ［ルール設定（サーバ公開）に戻る］をクリックする。

追加したルールが反映されたサーバ公開ルール一覧画面が表示されます。

ルール設定追加結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。



サーバ公開ルールの削除

不要になったサーバ公開ルールを削除することができます。

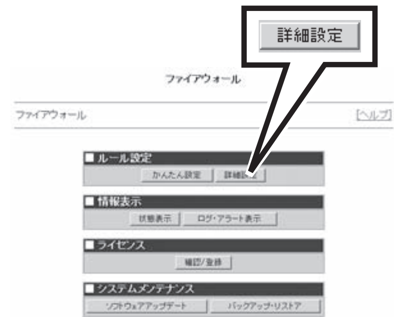
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

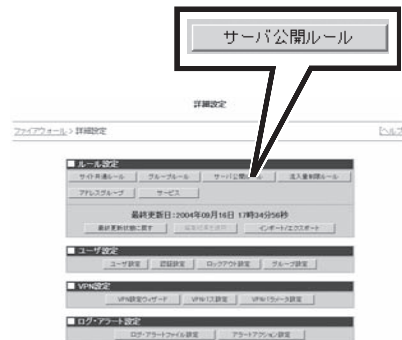
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。



詳細設定メニュー画面

4. 削除したいルールの「No.」の横に表示されるチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。





サーバ公開ルール一覧画面



- 一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、サーバ公開ルールの設定から削除することはできません。
- 「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。

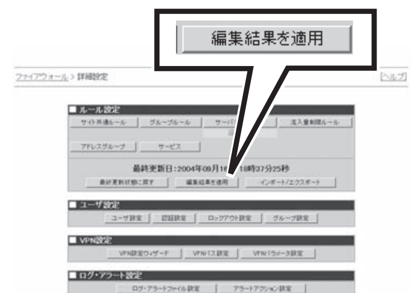
5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。



[キャンセル]をクリックすると、削除されずにサーバ公開ルール一覧画面に戻ります。

ルールが削除されたサーバ公開ルール一覧画面が表示されます。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。



サーバ公開ルールの更新

一度設定したサーバ公開ルールの内容を変更することができます。

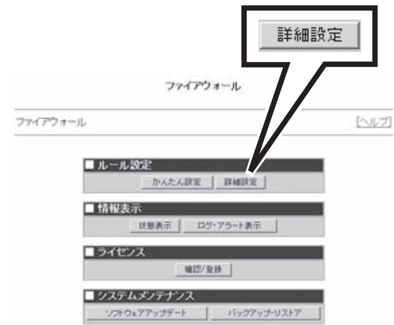
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

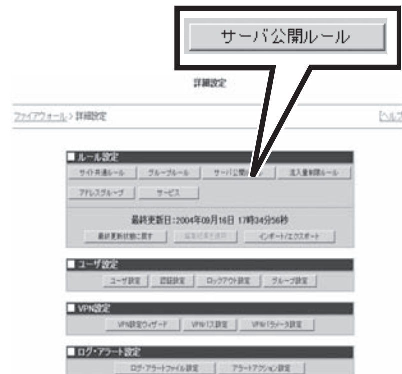
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。



詳細設定メニュー画面

4. 変更したいルールの「No.」をクリックする。

ルール設定更新画面が表示されます。



一覧の背景がピンク色の項目は、「かんたん設定ウィザード」を経由して設定されたルールであることを示しています。このルールについては、「記録」および「コメント」のみ変更することができます。その他の項目を更新する場合は、もう一度「かんたん設定ウィザード」に戻って設定をやり直してください。





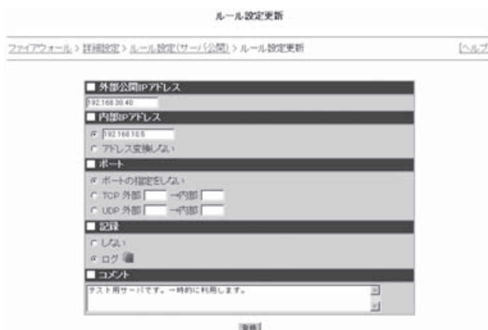
サーバ公開ルール一覧画面



「かんたん設定ウィザード」を用いてルールを再生成すると、「かんたん設定ウィザード」を経由して設定されたルールの「記録」および「コメント」の項目がデフォルト値（「記録」は［記録しない］、「コメント」は空欄）に戻ります。

通信ログを記録する必要がある場合やコメントを登録する場合は、「かんたん設定ウィザード」からではなく、詳細設定メニューの「ルール設定」よりルールを設定することを推奨します。

5. ルール設定更新画面に表示される各項目を入力する。



ルール設定更新画面

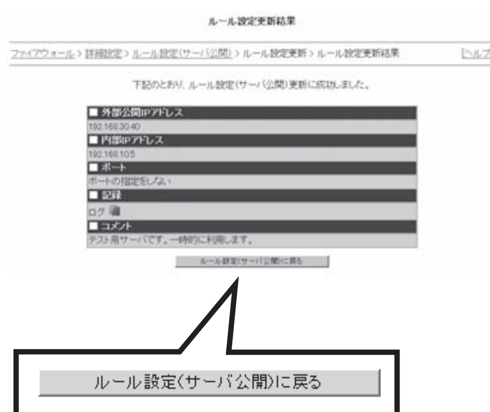
項　目	説　明
外部公開IPアドレス	外部ネットワークへ公開するIPアドレスを入力します。
内部IPアドレス	サーバの実際のIPアドレスを指定します。「外部公開IPアドレス」と異なる場合は、そのIPアドレスを入力します。
ポート	ポート番号の指定を行うかどうかを選択します。特定のポート番号についてのみ公開するか、ポート番号の変換を行う場合には、外部ネットワークへ公開するポート番号と、対応する内部ネットワークのポート番号を入力します。
記録	作成するルールに該当する通信パケットを検出したとき、ログ情報としてのみファイルに出力するか、それともファイルにはいっさい記録しないかを設定します。
コメント	任意のコメントを入力できます。最大で1000文字までを受け付けますが、右大不等号（<）および左大不等号（>）を含めることはできません。

6. ［登録］をクリックする。

ルール設定更新結果画面が表示されます。

7. ［ルール設定（サーバ公開）に戻る］をクリックする。

変更したルールが反映されたサーバ公開ルール一覧画面が表示されます。



ルール設定更新結果画面

8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で［登録］をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには［編集結果を適用］をクリックしてください。**
- **［最終更新状態に戻す］をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。**



詳細設定メニュー画面

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. ［詳細設定メニューに戻る］をクリックする。



外部から内部への通信におけるウェブ専用フィルタの設定

外部ネットワークから内部ネットワークへのHTTP通信のフィルタリング設定を行うことができます。ここでは、アクセス制御する端末やネットワークを設定することで外部ネットワークから内部ネットワークへのHTTP通信を制限します。

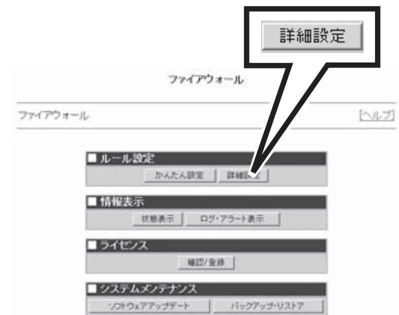
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

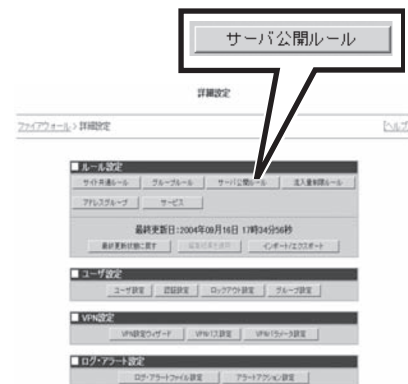
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サーバ公開ルール]をクリックする。

   サーバ公開ルール一覧画面が表示されます。



詳細設定メニュー画面

4. 「オプション」の「ウェブ専用フィルタ設定」をクリックする。

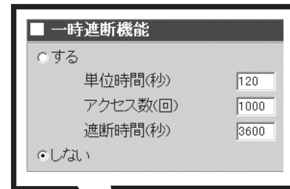
   ウェブ専用フィルタ設定(外→内)画面が表示されます。

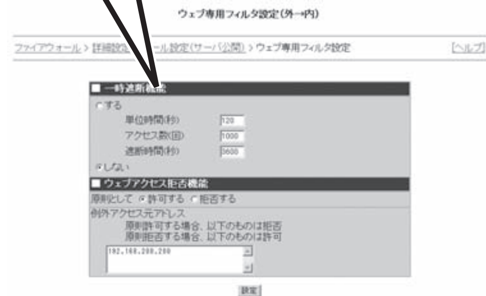


サーバ公開ルール一覧画面

5. 一時遮断機能の利用の有無を選択する。利用する場合は、単位時間、アクセス数、遮断時間を設定する。

> ヒント
>
> 一時遮断機能によって、外部ネットワークの特定の端末から内部ネットワーク上のウェブサーバに過剰アクセスする攻撃(DoS攻撃)を回避します。指定する単位時間あたり、指定するアクセス数を越えて接続した場合、その送信元からのウェブアクセスを指定した遮断時間の間制限します。
>
> さらに、一時遮断機能を有効にしていると、外部ネットワークの過剰な数の端末から内部ネットワーク上のウェブサーバにアクセスする攻撃(DDoS攻撃)についても回避します。この場合は指定する単位時間あたり、50を超える送信元からのウェブアクセスを制限します。

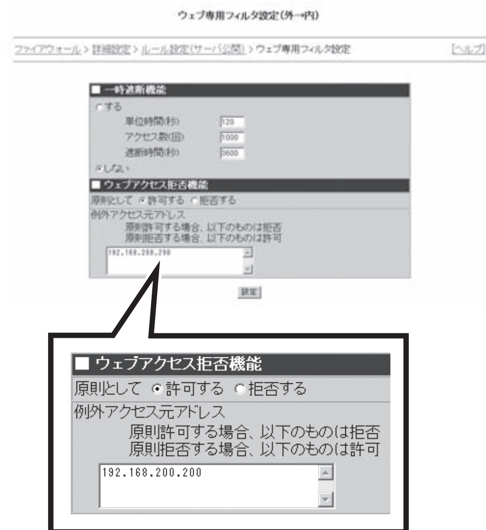




ウェブ専用フィルタ設定(外→内)画面

6. ウェブアクセス拒否機能を設定する。

- 原則として許可する
  ウェブサーバに対するアクセスを原則として許可する場合に選択します。例外として拒否するネットワーク、端末がある場合は、下に表示されるテキストエリアに拒否対象となるネットワークアドレスまたはIPアドレスを設定します。
- 原則として拒否する
  ウェブサーバに対するアクセスを原則として拒否する場合に選択します。例外として許可するネットワーク、端末がある場合は、下に表示されるテキストエリアに許可対象となるネットワークアドレスまたはIPアドレスを設定します。



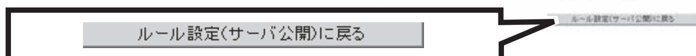
ウェブ専用フィルタ設定(外→内)画面

7. [設定]をクリックする。

ウェブ専用フィルタ設定(外→内)結果画面が表示されれます。

8. ［ルール設定（サーバ公開）に戻る］をクリックする。

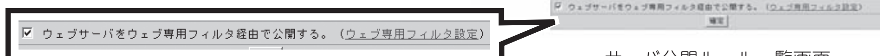
サーバ公開ルール一覧画面が表示されます。



ウェブ専用フィルタ設定（外→内）結果画面

9. 「ウェブサーバをウェブ専用フィルタ経由で公開する。」のチェックボックスにチェックし、［確定］をクリックする。

設定更新結果画面が表示されるので、［ルール設定（サーバ公開）に戻る］をクリックします。



サーバ公開ルール一覧画面

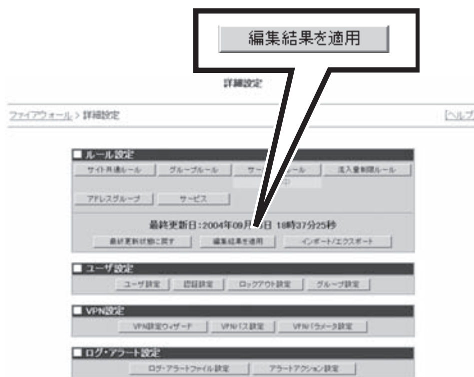
重要

確定をクリックしないと、ウェブ専用フィルタ設定をしてもフィルタリング機能は有効になりません。逆にウェブ専用フィルタ設定をしないでフィルタリング機能を有効にしても効果はありません。

10. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順9で［確定］をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには［編集結果を適用］をクリックしてください。**
- **［最終更新状態に戻す］をクリックすると、Express5800/SG300はフィルタリング機能の設定前の状態に戻ります。**



詳細設定メニュー画面

11. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

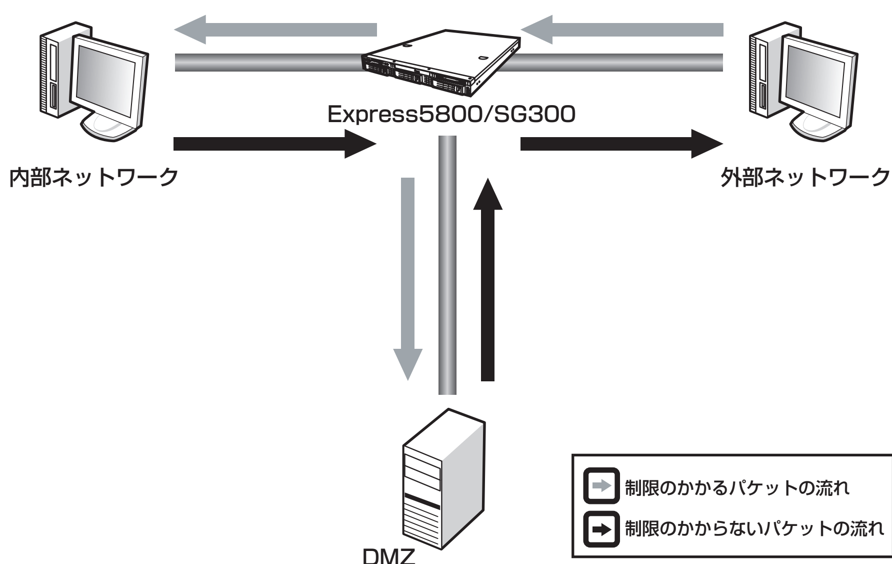
フィルタリング設定がExpress5800/SG300に適用され、設定結果画面が表示されます。

12. [詳細設定メニューに戻る]をクリックする。



流入量制限ルール

流入量制限ルールとは、各インタフェースを介して内部方向に流入するパケットを監視し、流入量が設定した値を超えた場合は、Express5800/SG300を越えての新規の接続要求を拒否する機能のことです。
パケット量は、宛先や送信元、ポートによらず、指定したインタフェースに流れる全パケットの総量を測ります。
なお、流入量制限は通信の片方向だけに掛かります。外部ネットワークからExpress5800/SG300へ流入する方向と、Express5800/SG300を経て内部ネットワーク/DMZへ流入する方向に制限をかける場合でも、内部ネットワーク/DMZから外部ネットワークへの通信は影響を受けません。
これにより、DoS攻撃などの過負荷となる通信から内部サーバを保護することができます。



流入量ルール制限

流入量制限ルールでは以下の項目を設定します。

- 流入量制限ルールの設定内容の確認
- 流入量制限ルールの追加
- 流入量制限ルールの削除
- 流入量制限ルールの更新

流入量制限ルールの設定内容の確認

Express5800/SG300は設定されたインタフェースの流入量を監視し、流入量の上限を超えると、ファイアウォールを越えての新規の接続要求を拒絶するようになります。



かんたん設定で不正アクセス対策レベルを「アドバンス」に設定した場合、外部からファイアウォールへのパケット流入量を70Mbpsに制限します。

流入方向や制限値は、流入量制限ルールで変更することができます。

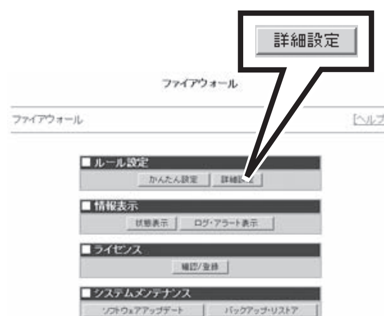
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



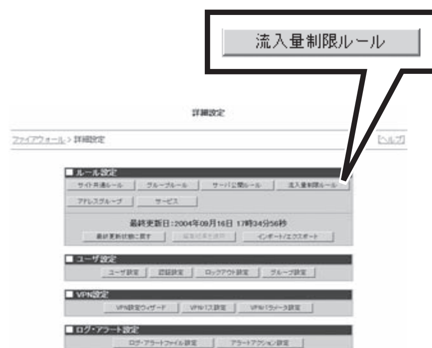
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[流入量制限ルール]をクリックする。



詳細設定メニュー画面

流入量制限ルール一覧画面が表示されます。表示される内容は以下の通りです。

項　目	説　明
No.	ルールの番号です。
流入方向	制限を掛ける流入方向を表示します。
制限値	指定する方向に流入するパケット量の上限値です。

ルール設定(流入量制限)

ファイアウォール > 詳細設定 > ルール設定(流入量制限)　[ヘルプ]

かんたん設定(ネットワーク構成)の確認

ルールの追加・削除・更新を行なった場合は、詳細設定トップ画面の「編集結果を適用」ボタンをクリックください。

一覧末尾にルールを [追加]
選択したルールを [削除]

No.	流入方向	制限値
☐ 1	ファイアウォール→DMZ(172.16.16.0/25)	10 Mbps
☐ 2	外部→ファイアウォール	10 Mbps

☐ 全選択/解除

流入量制限ルール一覧画面



画面右上の「かんたん設定(ネットワーク構成)の確認」をクリックすると、かんたん設定で設定した内容が別ウィンドウで表示されます。

具体的な流入量制限ルール一覧の事例を示します。

No.	流入方向	制限値
☐ 1	ファイアウォール→DMZ(172.16.16.0/25)	10 Mbps
☐ 2	外部→ファイアウォール	10 Mbps

流入量制限ルール一覧画面

ルールの1行目:　ファイアウォールからDMZへ流れるパケットの総流入量を10Mbpsに制限することを表します。

ルールの2行目:　外部ネットワークからファイアウォールへ流れるパケットの総流入量を10Mbpsに制限することを表します。

流入量制限ルールの追加

必要に応じて流入量制限ルールを追加することができます。

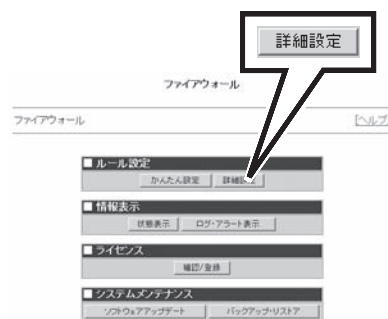
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

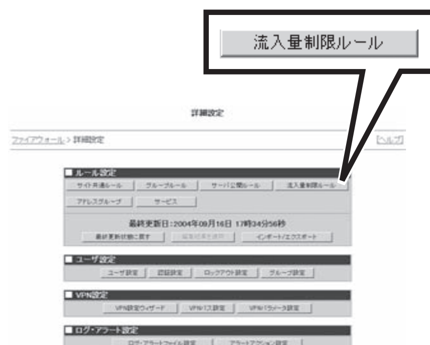
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[流入量制限ルール]をクリックする。

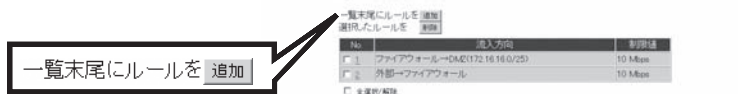
   流入量制限ルール一覧画面が表示されます。



詳細設定メニュー画面

4. 「一覧末尾にルールを『追加』」をクリックする。

   ルール設定追加画面が表示されます。



流入量制限ルール一覧画面

5. ルール設定追加画面に表示される各項目を設定する。

- 流入方向
  流入方向をラジオボタンで選択します。
- 制限
  指定した方向に流入するパケット量の上限値を設定します。Mbps単位による指定ができます。入力できる範囲は1から1000までです。



ルール設定追加画面

6. [登録]をクリックする。

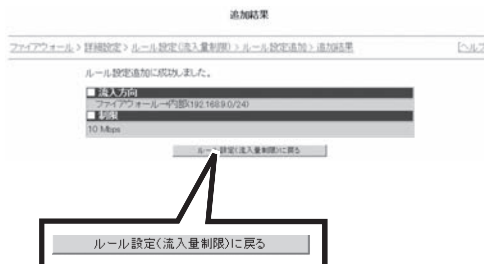
   追加結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

7. [ルール設定(流入量制限)に戻る]をクリックする。

   追加したルールが反映された流入量制限ルール画面が表示されます。



追加結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの追加前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. ［詳細設定メニューに戻る］をクリックする。



流入量制限ルールの削除

不要になった流入量制限ルールを削除することができます。

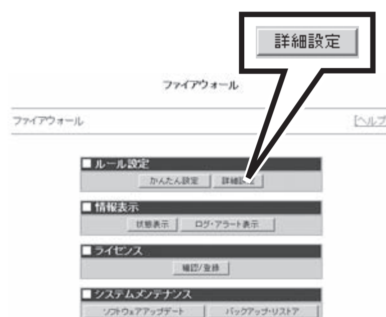
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから［ファイアウォール］をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から［詳細設定］をクリックする。

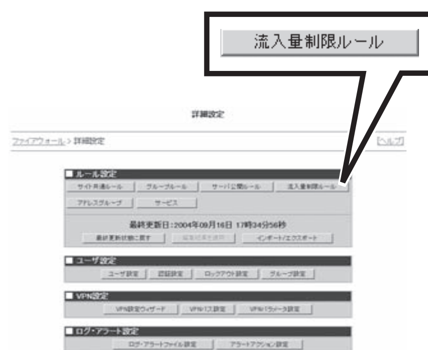
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から［流入量制限ルール］をクリックする。

   流入量制限ルール一覧画面が表示されます。

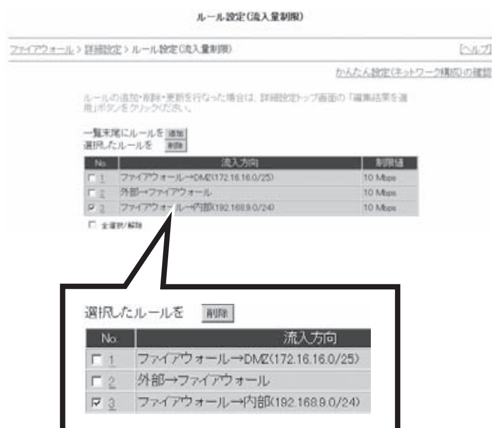


詳細設定メニュー画面

4. 削除したいルールの「No.」の横に表示されるチェックボックスをチェックし、「選択したルールを『削除』」をクリックする。



「全選択/解除」のチェックボックスをチェックすると、削除可能なルールのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのルールを削除対象から外すこともできます。



流入量制限ルール一覧画面

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。



[キャンセル]をクリックすると、削除されずに流入量制限ルール一覧画面に戻ります。

流入量制限ルールが削除され、削除を反映した流入量制限ルール一覧画面が表示されます。

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではルールの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はルールの削除前の状態に戻ります。**



詳細設定メニュー画面

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

ルールの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。



流入量制限ルールの更新

一度設定した流入量制限ルールの制限値を変更することができます。

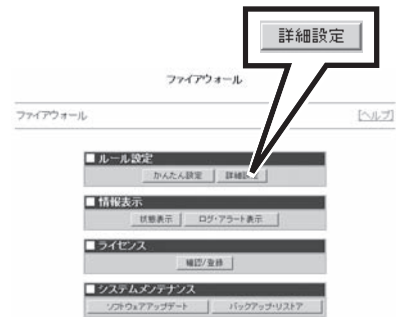
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

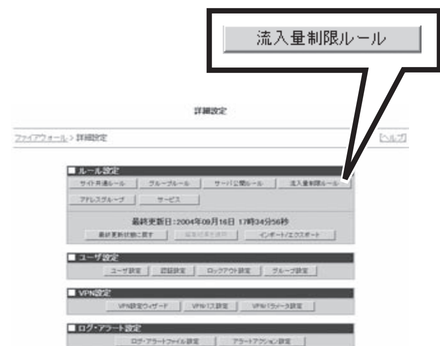
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[流入量制限ルール]をクリックする。

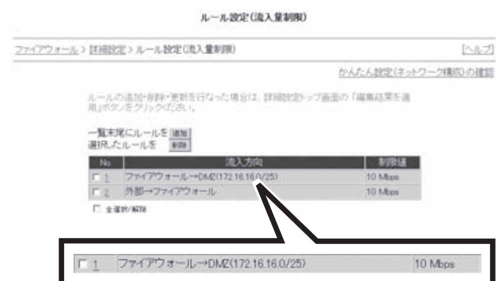
   流入量制限ルール一覧画面が表示されます。



詳細設定メニュー画面

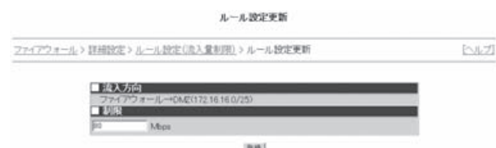
4. 変更したいルールの「No.」をクリックする。

   ルール設定更新画面が表示されます。



流入量制限ルール一覧画面

5. ルール設定更新画面からパケット流入量の制限値を設定する。



ルール設定更新画面

6. ［登録］をクリックする。

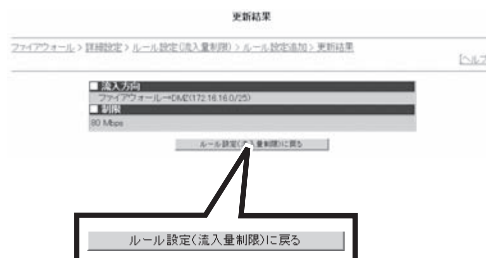
更新結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

7. ［ルール設定（流入量制限）に戻る］をクリックする。

更新したルールが反映された流入量制限ルール一覧画面が表示されます。



更新結果画面

8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で［登録］をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには［編集結果を適用］をクリックしてください。
- ［最終更新状態に戻す］をクリックすると、Express5800/SG300はルールの更新前の状態に戻ります。



詳細設定メニュー画面

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

更新したルールがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. ［詳細設定メニューに戻る］をクリックする。



アドレスグループ

アドレスグループとは、1つ以上のホストアドレスまたはネットワークアドレスをグループ化したもので、ユーザが自由に設定することができます。設定したアドレスグループはサイト共通ルール、グループルールのルール設定の際に送信元、宛先として指定することができます。これにより、簡単に環境に合わせたフィルタリング設定ができます。
アドレスグループは、ホスト、ネットワーク、ホストおよびネットワークを複数含むグループの3つに分けて考えることができます。
アドレスグループでは、以下のような設定・管理を行うことができます。

- アドレスグループの確認
- アドレスグループの追加
- アドレスグループの削除
- アドレスグループの更新

アドレスグループの確認

すでに設定したアドレスグループはアドレスグループ一覧画面から確認することができます。

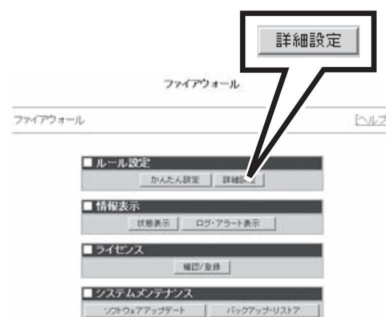
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



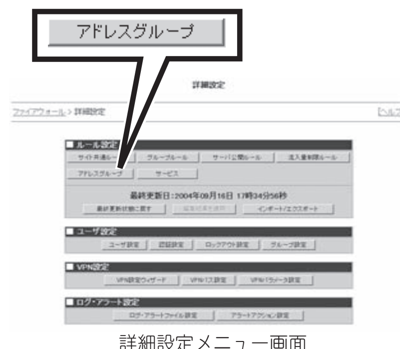
2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。



詳細設定メニュー画面

アドレスグループ一覧画面が表示されます。表示される内容は以下の通りです。

項　目	説　明	
名前	アドレスグループの種別を示すアイコンとアドレスグループの名称です。	
		（ホスト） 単一のホストアドレスを登録したときにこのアイコンを設定します。
		（ネットワーク） ネットワークアドレスを登録したときにこのアイコンを設定します。
		（グループ） ホストアドレス、ネットワークアドレスを複数登録したときにこのアイコンを設定します。
メンバ	設定したアドレスグループに所属するホストアドレス、ネットワークアドレスを表示します。	



アドレスグループ一覧画面

具体的なアドレスグループ一覧の事例を示します。

- 上記画面の部門ネット1

  ネットワークアドレス192.168.20.0/24のネットワークが登録されたアドレスグループです。

- 上記画面のウェブサーバ

  IPアドレス192.168.10.101のホストが登録されたアドレスグループです。

- 上記画面の東京営業所

  ネットワークアドレス192.168.128.0/17、192.168.100.0/24が登録されたアドレスグループです。

アドレスグループの追加

必要に応じてアドレスグループを追加することができます。

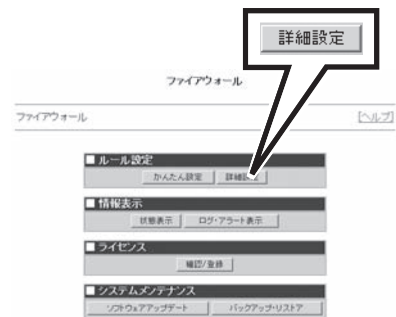
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

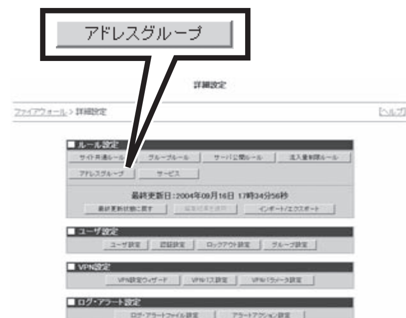
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。

   アドレスグループ一覧画面が表示されます。



詳細設定メニュー画面

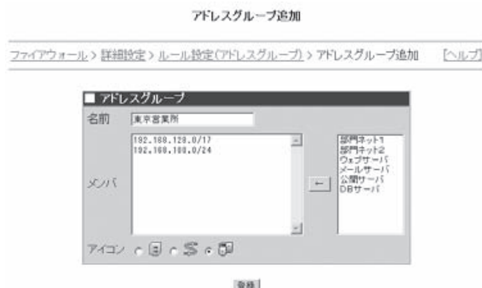
4. 「アドレスグループを『追加』」をクリックする。

   アドレスグループ追加画面が表示されます。



アドレスグループ一覧画面

5. アドレスグループ追加画面に表示される各項目を設定する。



アドレスグループ追加画面

項　目	説　明	
名前	アドレスグループの名称です。 最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字（日本語）も使用できます。既存のアドレスグループと重複する名前は付けられません。	
メンバ	設定するアドレスグループに所属するホストアドレス、ネットワークアドレスを登録します。 1行に1アドレスを入力します。 右側に既存のアドレスグループが表示されますので、アドレスグループを選択し、[←]をクリックすることでそのメンバを取り込むこともできます。	
アイコン		（ホスト） 単一のホストアドレスを登録したときにこのアイコンを設定します。
		（ネットワーク） ネットワークアドレスを登録したときにこのアイコンを設定します。
		（グループ） ホストアドレス、ネットワークアドレスを複数登録したときにこのアイコンを設定します。



- 同じアドレスを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- アドレスグループが含むことのできるメンバの数は、最大50個までです。

6. [登録]をクリックする。

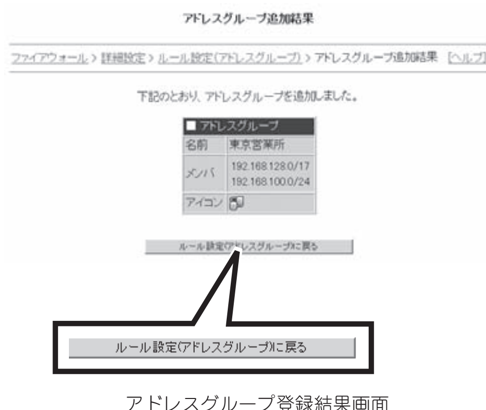
アドレスグループ登録結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

7. [ルール設定(アドレスグループ)に戻る]をクリックする。

   追加したアドレスグループが反映されたアドレスグループ一覧画面が表示されます。



アドレスグループ登録結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はアドレスグループの追加前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したアドレスグループがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。



アドレスグループの削除

不要になったアドレスグループを削除することができます。

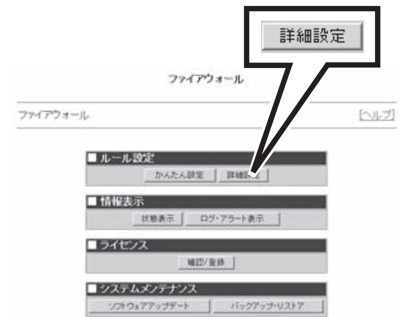
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

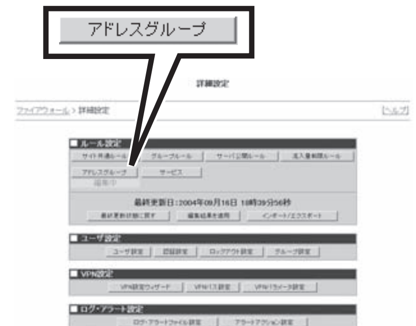
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。

   アドレスグループ一覧画面が表示されます。



詳細設定メニュー画面

ファイアウォール機能の設定方法

4. 削除したいアドレスグループの「名前」の横に表示されるチェックボックスをチェックし、「選択したアドレスグループを『削除』」をクリックする。



「全選択/解除」のチェックボックスをチェックすると、削除可能なアドレスグループのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのアドレスグループを削除対象から外すこともできます。

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。



[キャンセル]をクリックすると、削除されずにアドレスグループ一覧画面に戻ります。

アドレスグループが削除され、削除を反映したアドレスグループ一覧画面が表示されます。

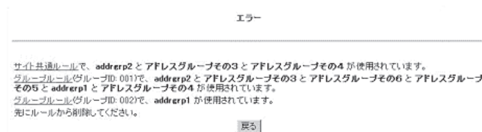


選択したアドレスグループが、サイト共通ルールまたはグループルールで指定されている場合、削除することができません。その場合、エラー内容を示す画面が表示されます。

エラーの説明文中に表示される、サイト共通ルール、グループルールのリンクをクリックすると、それぞれサイト共通ルール一覧画面、グループルール一覧画面が表示されます。先にルールからアドレスグループを削除し、再度アドレスグループの削除を行ってください。

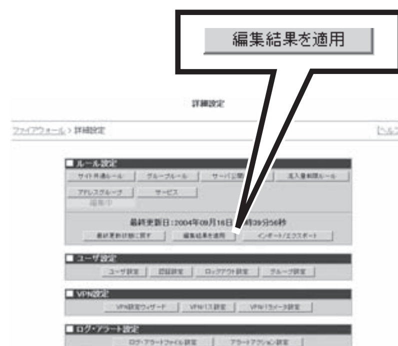


アドレスグループ一覧画面



エラー内容を示す画面

6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順5で[OK]をクリックしますが、この段階ではアドレスグループの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はアドレスグループの削除前の状態に戻ります。

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   アドレスグループの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。



アドレスグループの更新

一度設定したアドレスグループの内容を変更することができます。

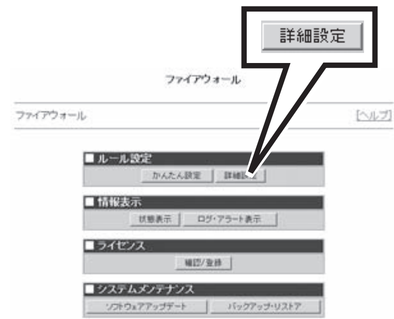
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

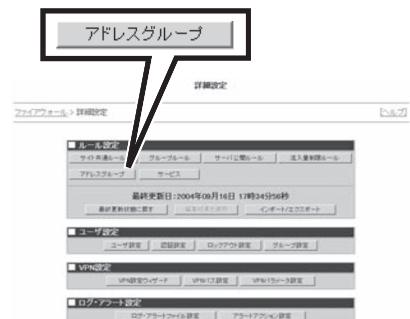
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[アドレスグループ]をクリックする。

   アドレスグループ一覧画面が表示されます。



詳細設定メニュー画面

4. 変更したいアドレスグループの「名前」をクリックする。

   アドレスグループ更新画面が表示されます。

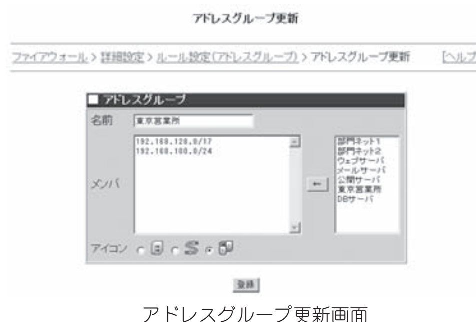


アドレスグループ一覧画面

5. アドレスグループ更新画面に表示される各項目を設定する。



- 同じアドレスを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- アドレスグループが含むことのできるメンバの数は、最大50個までです。



アドレスグループ更新画面

項　目	説　明	
名前	アドレスグループの名称です。 最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字（日本語）も使用できます。既存のアドレスグループと重複する名前は付けられません。	
メンバ	設定するアドレスグループに所属するホストアドレス、ネットワークアドレスを登録します。 1行に1アドレスを入力します。 右側に既存のアドレスグループが表示されますので、アドレスグループを選択し、[←]をクリックすることでそのメンバを取り込むこともできます。	
アイコン		（ホスト） 単一のホストアドレスを登録したときにこのアイコンを設定します。
		（ネットワーク） ネットワークアドレスを登録したときにこのアイコンを設定します。
		（グループ） ホストアドレス、ネットワークアドレスを複数登録したときにこのアイコンを設定します。

6. [登録]をクリックする。

   アドレスグループ更新結果画面が表示されます。

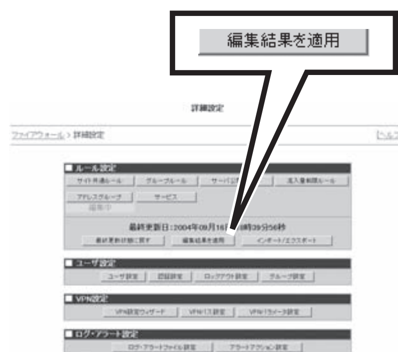
7. ［ルール設定（アドレスグループ）に戻る］をクリックする。

更新したアドレスグループが反映されたアドレスグループ一覧画面が表示されます。



アドレスグループ更新結果画面

8. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。



詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はアドレスグループの更新前の状態に戻ります。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

更新したアドレスグループがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. ［詳細設定メニューに戻る］をクリックする。



サービス

サービスとは、通信種別(プロトコル)ごとのタイプ指定(ポート番号、ICMPタイプなど)をグループ化したもので、ユーザが自由に設定することができます。設定したサービスはサイト共通ルール、グループルールの通信種別として指定することができます。これにより、簡単に環境に合わせたフィルタリング設定ができます。
サービスでは、以下のような設定管理を行うことができます。

- サービスの確認
- サービスの追加
- サービスの削除
- サービスの更新

サービスの確認

すでに設定したサービスや標準定義サービスはサービス一覧画面から確認することができます。

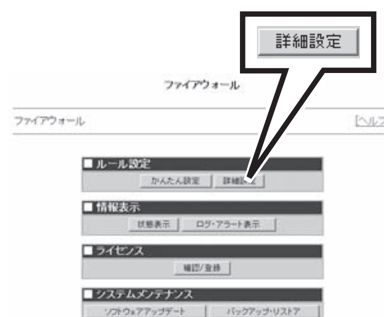
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。

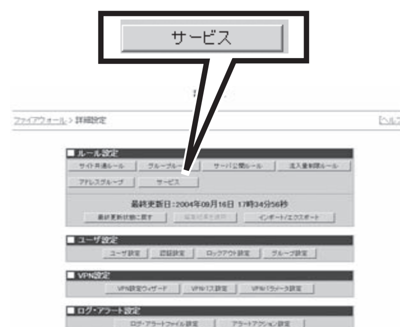


ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

   サービス一覧画面が表示されます。表示される内容は以下の通りです。

項　目	説　明
名前	サービスの名前です。
メンバ	サービスの種別を表示します。



詳細設定メニュー画面

 ヒント

「標準定義サービス」をクリックすると、あらかじめシステムで定義されたサービスの一覧を表示します。標準定義サービスはピンク色で表示され、変更・削除することができません。

「全サービス一覧」をクリックすると、ユーザ定義サービスと標準定義サービスを一覧表示します。

「ユーザ定義サービス」をクリックするとユーザ定義サービスの一覧を表示します。詳細設定メニューから画面を表示した場合は、ユーザ定義サービスの一覧が表示されています。

ルール設定（サービス）

ファイアウォール > 詳細設定 > ルール設定（サービス） [ヘルプ]

サービスを 追加
選択したサービスを 削除

ユーザ定義サービス一覧 標準定義サービス一覧 全サービス一覧

名前	メンバ
□ ウェブサービス	tcp/80, tcp/443
□ ファイル転送	tcp/21
□ アプリケーションA	tcp/50080
□ 共通サービス	tcp/25, tcp/80, tcp/443, tcp/110, tcp/53, udp/53, tcp/389

□全選択／解除

サービス一覧画面

具体的なサービス一覧の事例を示します。

上記画面のウェブサービス
TCPポート80のサービス（HTTP通信）、443のサービス（HTTPS通信）を含むサービスとして定義されています。

上記画面のファイル転送
TCPポート21のサービス（FTP通信）として定義されています。

上記画面のアプリケーションA
TCPポート50080のサービスとして定義されています。

上記画面の共通サービス
TCPポート25のサービス（SMTP通信）、80のサービス（HTTP通信）、443のサービス（HTTPS通信）、110のサービス（POP通信）、53のサービス（DNS通信）、389のサービス（LDAP通信）、UDPポート53のサービス（DNS通信）を含むサービスとして定義されています。

サービスの追加

必要に応じてサービスを追加することができます。

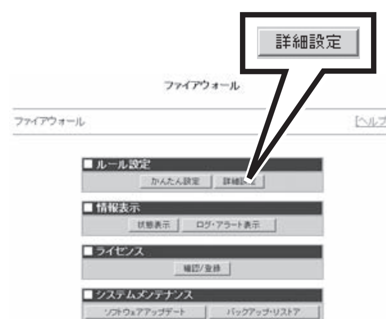
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

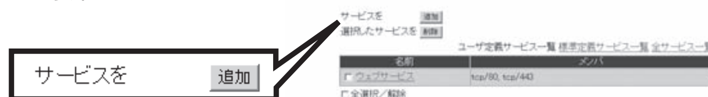
   サービス一覧画面が表示されます。



詳細設定メニュー画面

4. 「サービスを『追加』」をクリックする。

   サービス追加画面が表示されます。



サービス一覧画面

5. サービス追加画面に表示される各項目を設定する。



サービス追加画面

項　目	説　明	
名前	サービスの名称です。 最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字（日本語）も使用できます。既存のサービスと重複する名前は付けられません。	
メンバ	TCP/UDP	ラジオボタンを選択し、ポート番号を指定します。ハイフン(-)で区切って範囲を指定することができます。指定後、[←]をクリックすることで登録します。
	ICMP	ラジオボタンを選択し、右側のリストボックスからタイプを指定して[←]をクリックすることで登録します。
	定義済みサービス	ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。
	その他のプロトコル	ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。



- 同じメンバを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- サービスが含むことのできるメンバの数は、最大50個までです。

6. [登録]をクリックする。

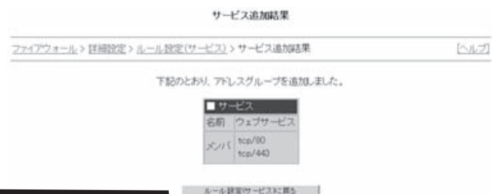
サービス追加結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

7. [ルール設定(サービス)に戻る]をクリックする。

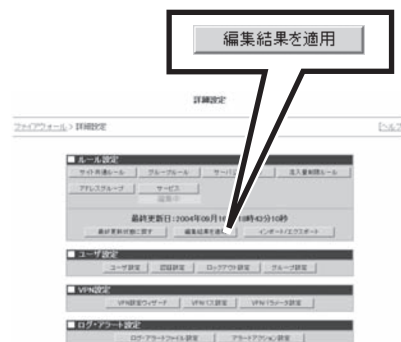
追加したサービスが反映されたサービス一覧画面が表示されます。



ルール設定(サービス)に戻る

サービス追加結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- **「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。**
- **[最終更新状態に戻す]をクリックすると、Express5800/SG300はサービスの追加前の状態に戻ります。**

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   新しく追加したサービスがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。



サービスの削除

不要になったユーザ定義サービスを削除することができます。
標準定義サービスは削除できません。

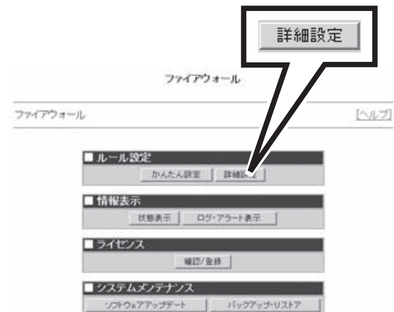
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

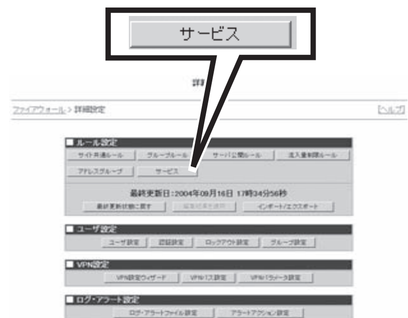
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

   サービス一覧画面が表示されます。

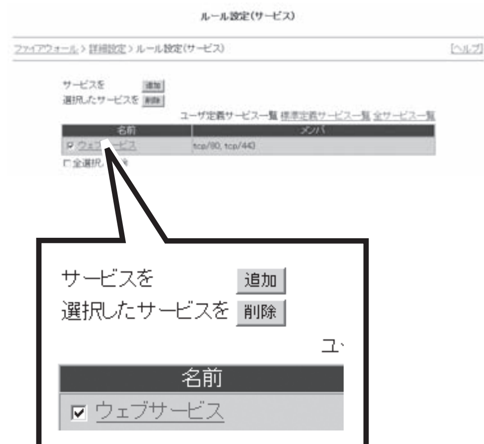


詳細設定メニュー画面

4. 削除したいサービスの「名前」の横に表示されるチェックボックスをチェックし、「選択したサービスを『削除』」をクリックする。



「全選択/解除」のチェックボックスをチェックすると、削除可能なサービスのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのサービスを削除対象から外すこともできます。



サービス一覧画面

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。



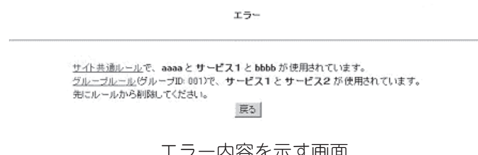
[キャンセル]をクリックすると、削除されずにサービス一覧画面に戻ります。

サービスが削除され、削除を反映したサービス一覧画面が表示されます。



選択したサービスが、サイト共通ルールまたはグループルールで指定されている場合、削除することができません。その場合、エラー内容を示す画面が表示されます。

エラーの説明文中に表示される、サイト共通ルール、グループルールのリンクをクリックすると、それぞれサイト共通ルール一覧画面、グループルール一覧画面が表示されます。先にルールからサービスを削除し、再度サービスの削除を行ってください。



エラー内容を示す画面

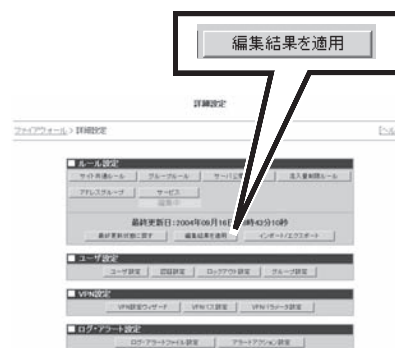
6. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。

  手順5で[OK]をクリックしますが、この段階ではサービスの削除はExpress5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。

- [最終更新状態に戻す]をクリックすると、Express5800/SG300はサービスの削除前の状態に戻ります。

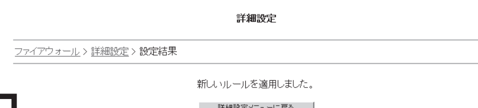


詳細設定メニュー画面

7. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   サービスの削除がExpress5800/SG300に適用され、設定結果画面が表示されます。

8. [詳細設定メニューに戻る]をクリックする。



サービスの更新

一度設定したサービスの内容を変更することができます。
標準定義サービスは変更できません。

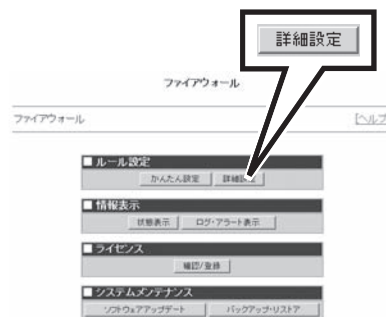
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

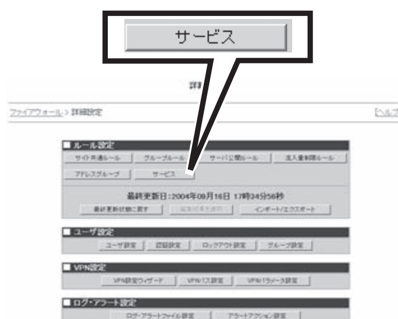
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サービス]をクリックする。

   サービス一覧画面が表示されます。



詳細設定メニュー画面

4. 変更したいサービスの「名前」をクリックする。

   サービス更新画面が表示されます。



サービス一覧画面

5. サービス更新画面に表示される各項目を設定する。



サービス更新画面

項　目	説　明	
名前	サービスの名称です。 最大で32バイトまでの英数文字列、ハイフン(-)、アンダースコア(_)が使用できます。全角文字（日本語）も使用できます。既存のサービスと重複する名前は付けられません。	
メンバ	TCP/UDP	ラジオボタンを選択し、ポート番号を指定します。指定後、[←]をクリックすることで登録します。
	ICMP	ラジオボタンを選択し、右側のリストボックスからタイプを指定して[←]をクリックすることで登録します。
	定義済みサービス	ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。
	その他のプロトコル	ラジオボタンを選択し、右側のリストボックスから選択して[←]をクリックすることで登録します。



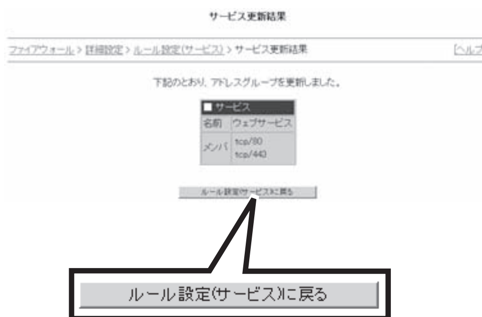
- 同じメンバを複数登録した場合は、2つ目以降が自動的に削除されて登録されます。
- サービスが含むことのできるメンバの数は、最大50個までです。

6. [登録]をクリックする。

   サービス更新結果画面が表示されます。

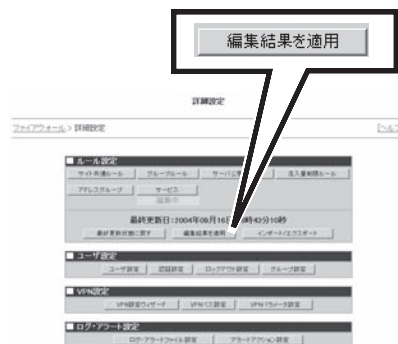
7. [ルール設定(サービス)に戻る]をクリックする。

   更新したサービスが反映されたサービス一覧画面が表示されます。



サービス更新結果画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



詳細設定メニュー画面

重要

- 「ルール設定」の中で、下に「編集中」と表示されている項目は、各項目の設定内容が編集中であることを示します。手順6で[登録]をクリックしますが、この段階では新しい設定内容を登録しただけで、Express5800/SG300には適用されていない状態であるため、詳細設定メニューには「編集中」と表示されます。作成した設定内容を適用するには[編集結果を適用]をクリックしてください。
- [最終更新状態に戻す]をクリックすると、Express5800/SG300はサービスの更新前の状態に戻ります。

9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   更新したサービスがExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。



ルール設定の履歴表示

「かんたん設定」や詳細設定メニューの「ルール設定」で設定できる各種ルールは、設定変更するたびに設定情報が履歴として保持されます。この履歴情報を利用することで、過去の設定内容を確認したり、日時を指定してその時点の設定内容に戻したりすることができます。

- 設定履歴を参照するには
- 過去の設定内容に戻すには
- 設定履歴を削除するには

設定履歴を参照するには

日時を指定して設定した内容を参照することができます。

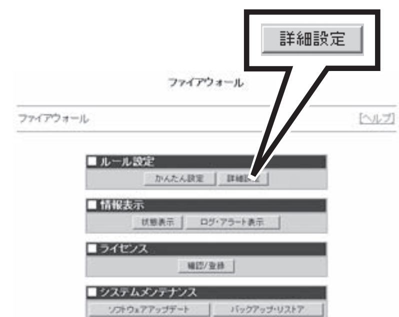
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

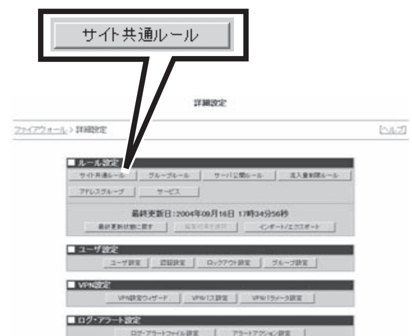
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

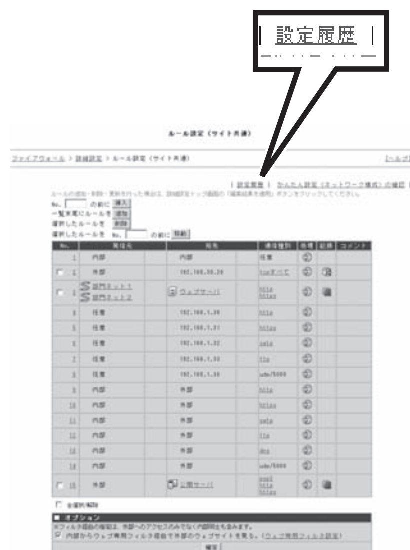
   サイト共通ルール設定一覧画面が表示されます。



詳細設定メニュー画面

4. 画面右上の「設定履歴」をクリックする。

   設定履歴参照画面が別ウィンドウで表示されます。



サイト共通ルール設定一覧画面

5. 「履歴日時」のプルダウンメニューを利用して表示したい日時を選択し、[表示する]をクリックする。

   指定した日時の履歴が表示されます。プルダウンメニューの下に現在表示している設定履歴の更新時間が表示されます。



設定履歴参照画面



ウィンドウを開いた直後は、その時点でもっとも新しい履歴が表示されます。

6. 「かんたん設定」、「サイト共通ルール」、「グループルール」、「サーバ公開ルール」、「流入量制限ルール」、「アドレス・サービス」のうち確認したい設定項目のタブをクリックする。

   それぞれの設定履歴が表示されます。

過去の設定内容に戻すには

指定した設定履歴の内容に設定を戻すことができます。

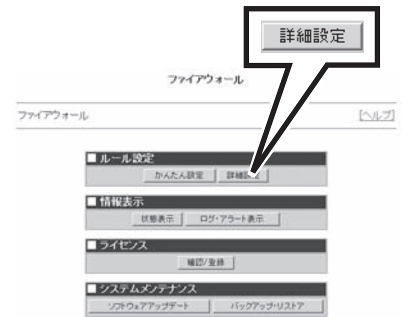
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

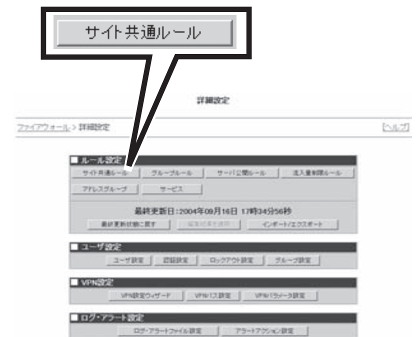
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   サイト共通ルール設定一覧画面が表示されます。



詳細設定メニュー画面

4. 画面右上の「設定履歴」をクリックする。

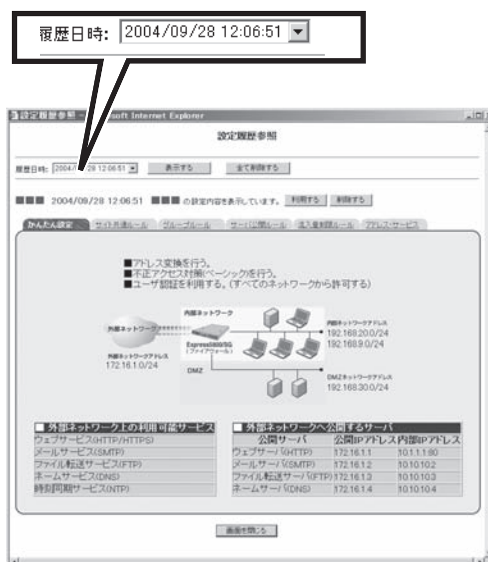
   設定履歴参照画面が別ウィンドウで表示されます。



サイト共通ルール設定一覧画面

5. 「履歴日時」のプルダウンメニューを利用して表示したい日時を選択し、［表示する］をクリックする。

   指定した日時の履歴が表示されます。プルダウンメニューの下に現在表示している設定履歴の更新時間が表示されます。



設定履歴参照画面



設定履歴参照画面を開いた直後は、その時点でもっとも新しい履歴が表示されます。

6. 「かんたん設定」、「サイト共通ルール」、「グループルール」、「サーバ公開ルール」、「流入量制限ルール」、「アドレス・サービス」のうち確認したい設定項目のタブをクリックする。

   それぞれの設定履歴が表示されます。

7. ［利用する］をクリックする。



設定履歴参照画面

8. 別ウィンドウで利用確認ダイアログメッセージが表示されるので[OK]をクリックする。

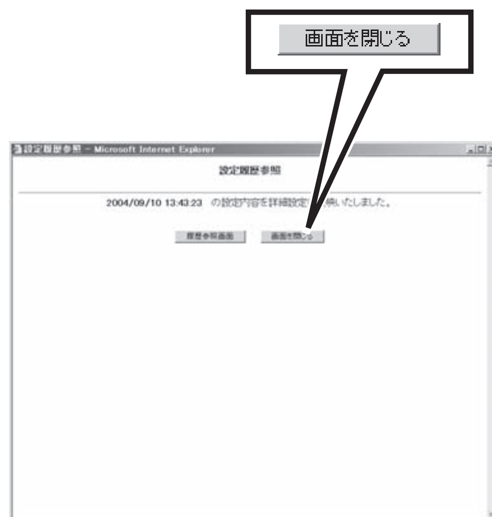
重要

このとき、指定した日時のすべての設定履歴情報が反映されます。

チェック

このとき、詳細設定を編集中の場合は確認画面が表示されます。
［戻る］をクリックすると、設定履歴の反映を行わないで元の画面に戻ります。
［次へ］をクリックすると、設定中の詳細設定データを破棄して、設定履歴の反映に進みます。

9. 設定履歴参照画面は、反映結果が表示される。再度設定履歴を表示する場合は、［履歴参照画面］をクリック、設定履歴参照画面を閉じる場合は［画面を閉じる］をクリックする。



設定履歴参照画面

10. 詳細設定メニューに戻り、［編集結果を適用］をクリックする。



11. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、［OK］をクリックする。

設定履歴がExpress5800/SG300に適用され、設定結果画面が表示されます。

12. ［詳細設定メニューに戻る］をクリックする。



設定履歴を削除するには

設定履歴を削除することができます。

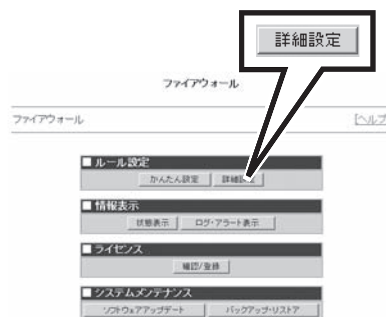
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

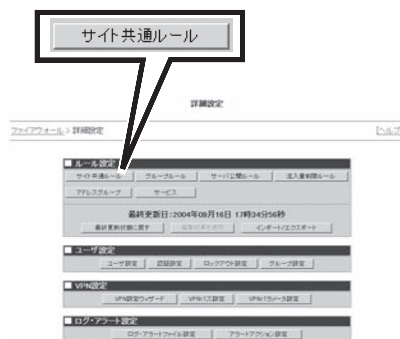
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

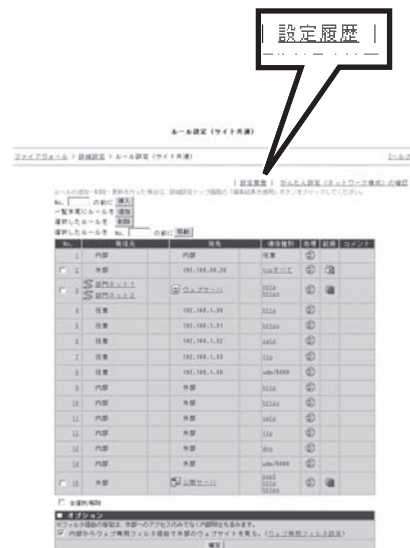
3. 詳細設定メニューの「ルール設定」から[サイト共通ルール]をクリックする。

   サイト共通ルール設定一覧画面が表示されます。



詳細設定メニュー画面

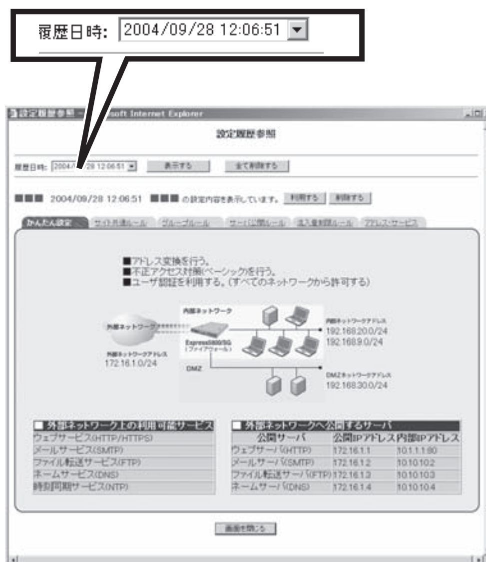
4. 画面右上の「設定履歴」をクリックすると、設定履歴参照画面が別ウィンドウで表示される。



サイト共通ルール設定一覧画面

5. 「履歴日時」のプルダウンメニューを利用して表示したい日時を選択し、［表示する］をクリックする。

指定した日時の履歴が表示されます。プルダウンメニューの下に現在表示している設定履歴の更新時間が表示されます。



設定履歴参照画面



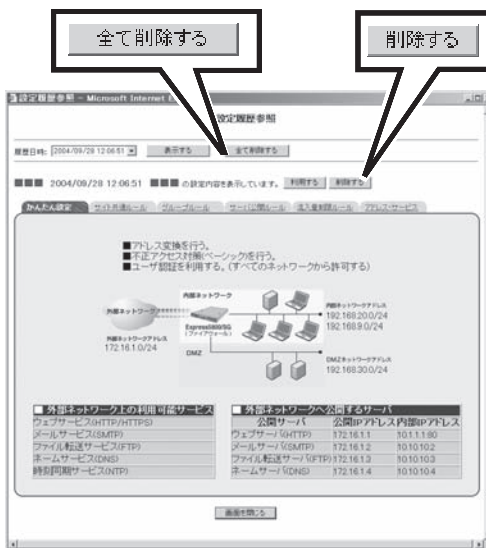
設定履歴参照画面を開いた直後は、その時点でもっとも新しい履歴が表示されます。

6. 「かんたん設定」、「サイト共通ルール」、「グループルール」、「サーバ公開ルール」、「流入量制限ルール」、「アドレス・サービス」のうち確認したい設定項目のタブをクリックする。

それぞれの設定履歴が表示されます。

7. ［削除する］または［全て削除する］をクリックする。

［削除する］をクリックした場合は、表示中の日時の設定履歴を削除します。
［全てを削除する］をクリックした場合は、すべての設定履歴を削除します。



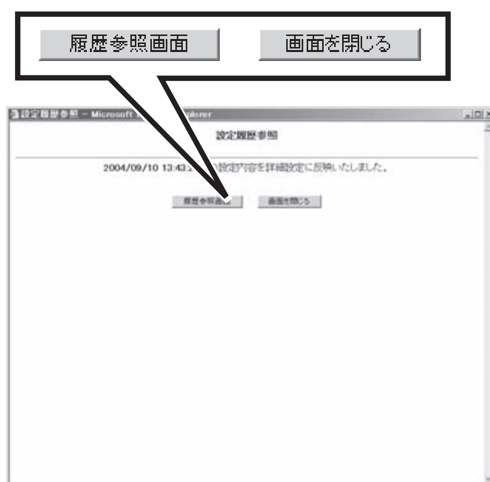
設定履歴参照画面

8. 別ウィンドウで利用確認ダイアログメッセージが表示されるので[OK]をクリックする。

[削除する]をクリックした場合は、設定履歴参照画面に反映結果が表示される。

9. 再度設定履歴を表示する場合は[履歴参照画面]を、設定履歴参照画面を閉じる場合は[画面を閉じる]をクリックする。

[全てを削除する]をクリックした場合は、設定履歴参照画面に反映結果が表示さます。設定履歴参照画面を閉じる場合は[画面を閉じる]をクリックしてください。



設定履歴参照画面

インポート/エクスポート

詳細設定メニューの「ルール設定」で設定できる「サイト共通ルール」、「サーバ公開ルール」、「流入量制限ルール」、「サービス」、「アドレスグループ」の設定内容を記述したファイルをExpress5800/SG300からエクスポートしたり、インポートしたりすることができます。

- 設定内容のインポート
- 設定内容のエクスポート

設定内容のインポート

詳細設定メニューの「ルール設定」で設定できる「サイト共通ルール」、「サーバ公開ルール」、「流入量制限ルール」、「サービス」、「アドレスグループ」の設定内容を記述したファイルをExpress5800/SG300にインポートすることができます。

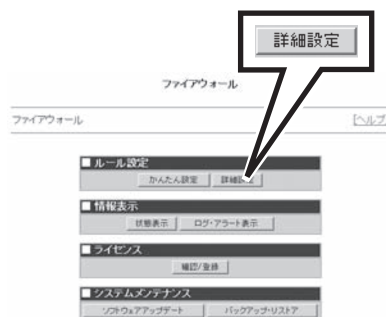
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

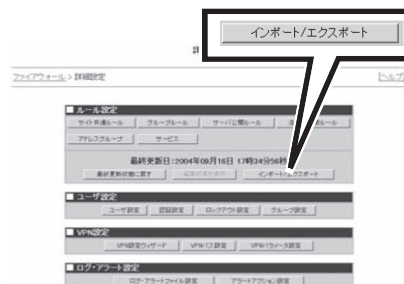
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[インポート/エクスポート]をクリックする。

   インポート/エクスポート画面が表示されます。



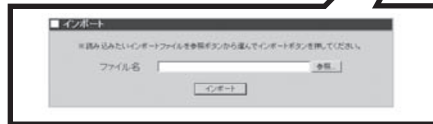
詳細設定メニュー画面

ファイアウォール機能の設定方法

4. [参照]をクリックしてインポートしたいファイルを指定し、[インポート]をクリックする。

インポートファイル内容確認画面が表示されます。各タブをクリックすると、設定内容が表示されます。






チェック

- ファイルのインタフェース情報が異なる場合は、インポートできません。エラーメッセージが表示され、[利用する]は使用できなくなります。
- ユーザが設定した「アドレスグループ」、「サービス」を利用してグループルールを設定している場合に、そのアドレスグループ、サービスが登録されていないファイルをインポートするとエラーになります。
- グループルールはインポート対象外です。

5. [利用する]をクリックする。

6. 別ウィンドウで確認ダイアログメッセージが表示されるので[OK]をクリックする。

インポート結果確認画面が表示されます。

利用する



7. [インポート/エクスポートに戻る]をクリックする。

インポート/エクスポートに戻る

インポート結果確認画面

8. 詳細設定メニューに戻り、[編集結果を適用]をクリックする。



9. 別ウィンドウで編集結果適用確認のダイアログメッセージが表示されるので、[OK]をクリックする。

   インポートしたファイルの内容がExpress5800/SG300に適用され、設定結果画面が表示されます。

10. [詳細設定メニューに戻る]をクリックする。



設定内容のエクスポート

詳細設定メニューの「ルール設定」で設定できる「サイト共通ルール」、「サーバ公開ルール」、「流入量制限ルール」、「サービス」、「アドレスグループ」の設定内容をファイルにエクスポートすることができます。

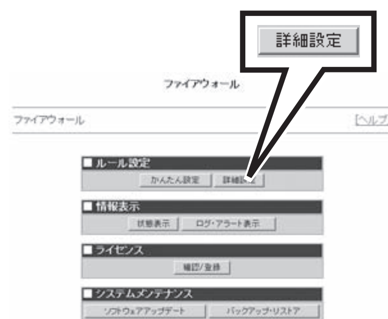
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

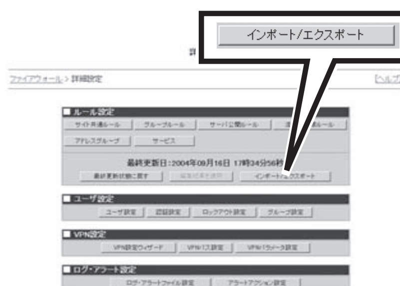
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ルール設定」から[インポート/エクスポート]をクリックする。

   インポート/エクスポート画面が表示されます。



詳細設定メニュー画面

4. [エクスポート]をクリックする。

   ファイルのダウンロード画面が表示されます。保存をクリックして、保存先を指定します。



ユーザ設定

Express5800/SG300を利用してネットワークにアクセスするユーザの管理を行うことができます。
ユーザ設定では、以下の項目を設定/管理します。

ユーザ設定 ....Express5800/SG300が管理するユーザの登録、削除、変更が行えます。

認証設定 ....ユーザ認証を利用するかどうかを設定します。

ロックアウト設定 ....ユーザ認証のエラーの上限を設定し、設定値を超えて認証に失敗したユーザはアクセスできないようにします。

グループ設定 ....ユーザをグループに分けて登録・管理することができます。

ユーザ設定

Express5800/SG300を利用したユーザ管理では、以下のような設定・管理を行うことができます。

- ユーザ情報の確認
  Express5800/SG300が管理するユーザ情報を表示します。
- CSVファイルを経由したユーザの一括登録
  CSVファイルに記録したユーザ情報を読み込んで登録します。
- ユーザの個別追加
  ユーザを個別に登録します。
- ユーザ情報の削除
  登録したユーザ情報を削除します。
- ユーザ情報の更新
  登録済みのユーザ情報の内容を修正します。
- ユーザ情報のCSVファイルへの出力
  登録されているユーザ情報をCSVファイルに出力します。

ユーザ情報の確認

登録されているユーザ情報を確認することができます。

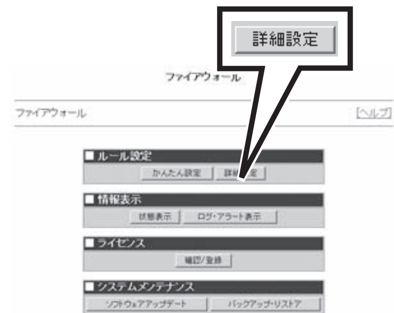
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

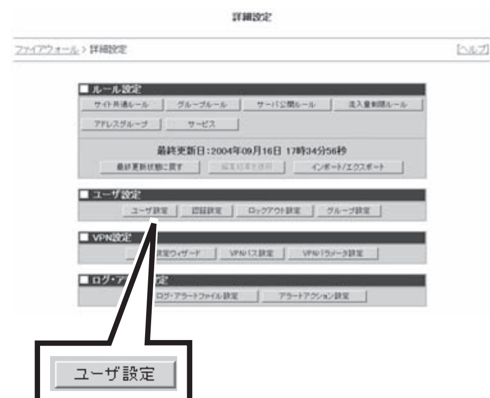
3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

   ユーザ情報一覧画面が表示されます。表示される内容は以下の通りです。

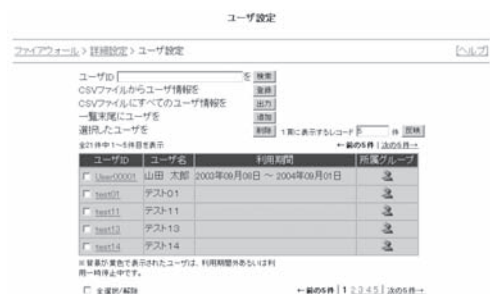
   - ユーザID
     登録されているユーザIDです。
   - ユーザ名
     登録されているユーザの名前です。
   - 利用期間
     利用可能な期間です。
   - 所属グループ
     アイコンをクリックするとグループの詳細情報を確認することができます。



ユーザ情報の一覧において、背景が黄色のユーザは、利用できないユーザであることを表しています。利用できないユーザとは、利用期間外となっているか、利用一時停止となっているユーザを指します。



詳細設定メニュー画面



ユーザ情報一覧画面



- ユーザIDからユーザ情報を検索するには、ユーザ情報をテキストボックスに入力し[検索]をクリックします。指定したユーザIDのユーザが表示されます。
- 「1頁に表示するレコード」の入力フィールドに件数を入力し、[反映]をクリックすると、その指定した件数でユーザ情報を一覧表示します。

ユーザ情報一覧画面

CSVファイルを経由したユーザの一括登録

あらかじめユーザ情報をCSVファイルで作成しておけば、CSVファイルを読み込ませることでユーザを一括登録することができます。

作成するCSVファイルは以下のようなフォーマットで作成します。これ以外のフォーマットでは、正しく読み込むことができません。

ユーザID,認証方式,パスワード,システム情報,システム情報,利用一時停止フラグ,システム情報,利用開始年月日,利用停止年月日,ユーザ名,備考



データの途中に不要なスペースなどは入れないでください。不要なスペースが入っていると正しく読み込めない場合があります。

カラム	項目	入力規則	必須/任意
1	ユーザID	最大で256バイトまでの英数文字列、ハイフン（-）、アンダースコア（_）、アットマーク（@）、ピリオド（.）が使用できます。	必須
2	認証方式	現在はpasswordに固定です。	必須
3	パスワード	6バイト以上256バイト以内の英数文字列で指定します。 平分でパスワードを登録するときは、パスワードのみを指定してください。ハッシュされたパスワードを指定する場合は、先頭に"{SHA1}"とつけて登録します。取得したCSVファイルでは、ハッシュされたパスワードが指定されます。	必須
4	システム情報	空白を指定してください。 取得したCSVファイルを利用する場合は、編集しないで下さい。	任意
5	システム情報	空白を指定してください。 取得したCSVファイルを利用する場合は、編集しないで下さい。	任意
6	利用一時停止フラグ	0は利用可、1は利用不可です。 値が1のときはユーザ認証に失敗します。省略した場合は利用可（0を指定した場合と同じ）となります。	任意

カラム	項目	入力規則	必須/任意
7	システム情報	空白を指定してください。 取得したCSVファイルを利用する場合は、編集しないで下さい。	任意
8	利用開始年月日	YYYY/MM/DD形式で入力してください。 省略した場合は利用開始制限無しとなります。	任意
9	利用停止年月日	YYYY/MM/DD形式で入力してください。 省略した場合は利用停止制限無しとなります。	任意
10	ユーザ名	最大で128バイトまで指定できます。 カンマ(,)、ダブルクォーテーション(")、改行は使用できません。	必須
11	備考	最大で2048バイトまで指定できます。 カンマ(,)、ダブルクォーテーション(")は使用できません。	任意



読み込むCSVファイルは、ファイアウォールが動作している機器上ではなく、Management Consoleを表示している管理クライアント上に保存してください。

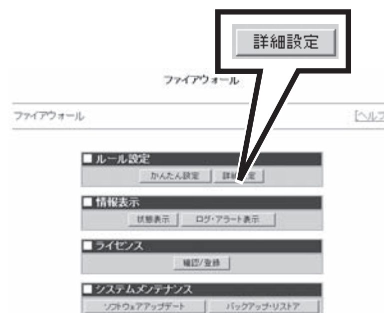
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

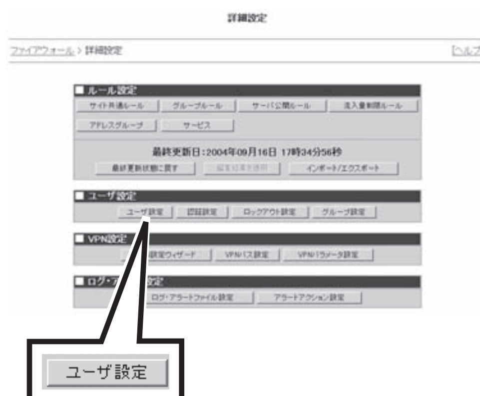
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

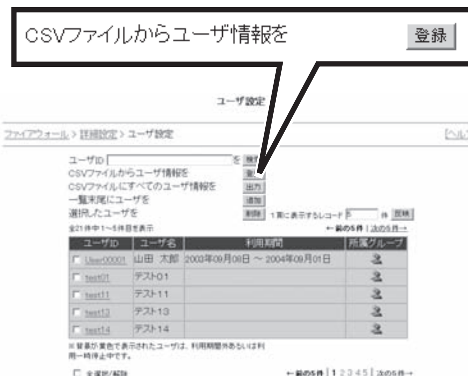
   ユーザ情報一覧画面が表示されます。



詳細設定メニュー画面

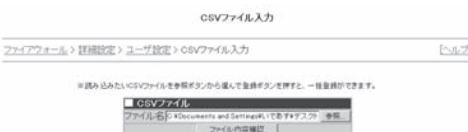
4. 「CSVファイルからユーザ情報を『登録』」をクリックする。

   CSVファイル入力画面が表示されます。



5. テキストボックス内に直接ファイル名を入力するか、[参照]をクリックし、管理クライアントに保存されているファイルの中から該当ファイルを指定する。ファイルを指定したら[ファイル内容確認]をクリックする。

   指定されたファイル内容が解析され、CSVファイル入力候補一覧画面が表示されます。



CSVファイル入力画面

6. CSVファイルと既に登録されたユーザ情報の中に重複データがある場合は、「重複ユーザは上書き登録する」または「重複ユーザは登録しない」のどちらかのラジオボタンをクリックする。



背景が黄色のユーザ情報は、CSVファイルの解析に失敗したレコードであることを示します。このレコードのデータは、ユーザ情報登録の対象とはしません。



CSVファイル入力候補一覧画面

7. [登録]をクリックする。

   CSVファイル入力結果画面が表示されます。



[キャンセル]をクリックすると、CSVファイル入力画面に戻ります。

8. CSVファイル入力結果画面を確認し、[ユーザ設定に戻る]をクリックする。



チェック

- 背景が黄色で色づけされたユーザ情報は、登録に失敗したレコードであることを示します。
- 背景が緑色で色づけされたユーザ情報は、すでに登録されていたレコードのため、登録を行わなかったことを示します。

ユーザ情報一覧画面に戻ります。このとき、新しく登録されたユーザ情報が一覧に反映された形で表示されます。

ユーザ設定に戻る

CSVファイル入力結果画面

ユーザの個別追加

ユーザ情報を個別に追加することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

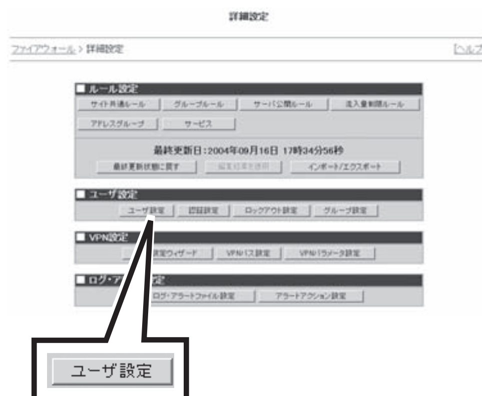
   詳細設定メニュー画面が表示されます。

詳細設定

ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から［ユーザ設定］をクリックする。

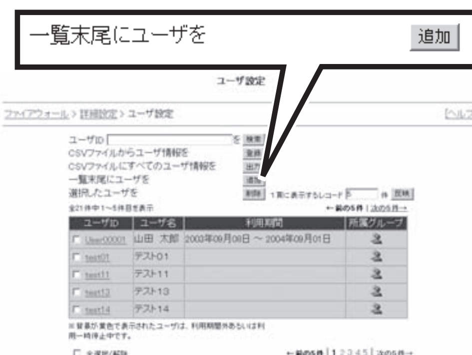
ユーザ情報一覧画面が表示されます。



詳細設定メニュー画面

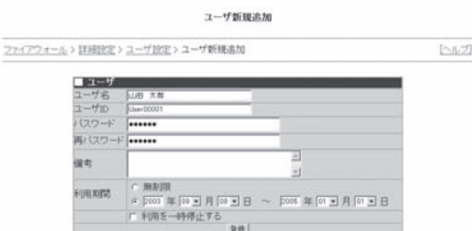
4. 「一覧末尾にユーザを『追加』」をクリックする。

ユーザ情報追加画面が表示されます。



ユーザ情報一覧画面

5. ユーザ情報追加画面に表示される各項目を入力する。



ユーザ情報追加画面

- ユーザ名（必須項目）
  追加するユーザを表す名称を入力します。最大で128バイトまでの任意の文字列を受け付けます。ただし、二重引用符（"）とカンマ（,）を含めることはできません。

- ユーザID（必須項目）
  追加するユーザを一意に表すIDを入力します。最大で256バイトまでの英数文字列、ハイフン（-）、アンダースコア（_）、アットマーク（@）、ピリオド（.）を受け付けます。ただし、二重引用符（"）とカンマ（,）を含めることはできません。すでに同じユーザIDの情報が登録されている場合には、登録に失敗します。

- パスワード（必須項目）
  追加するユーザのパスワードを入力します。6バイトから256バイトまでの英数文字列を受け付けます。

- 再パスワード（必須項目）
  追加するユーザのパスワードをもう一度入力します。

- 備考
  追加するユーザに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

- 利用期間
  追加するユーザの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、追加するユーザはログインできません。

- 利用を一時停止する
  運用上の理由などにより、追加するユーザの利用を一時停止したい場合、このチェックボックスにチェックをつけます。

6. ［登録］をクリックする。

   ユーザ情報追加結果画面が表示されます。

   ユーザ情報の登録内容が入力規則に違反している場合は、エラー内容を示す画面が表示されます。

ユーザ情報追加画面

7. 所属グループを設定する場合は、［所属グループ設定へ］をクリックする。所属グループ設定画面が表示されるので、所属グループ一覧から所属するグループのチェックボックスをチェックし、［登録］をクリックする。

   所属グループ設定結果画面が表示されます。

ユーザ情報追加結果画面

8. 所属グループを設定しない場合は、ユーザ情報追加結果画面の［ユーザ設定に戻る］をクリックする。

   所属グループを設定した場合は、所属グループ登録結果画面の［ユーザ設定に戻る］をクリックする。
   ユーザ情報一覧画面に戻ります。このとき、新しく登録されたユーザ情報が一覧に反映された形で表示されます。

   所属グループを設定するには、あらかじめ「グループ設定」をする必要があります。「グループ設定」については、231ページを参照してください。

所属グループ設定結果画面

ユーザ情報の削除

利用権限のなくなったユーザを削除することができます。

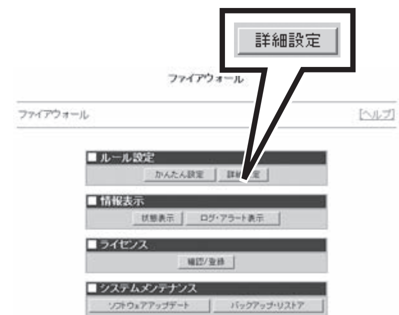
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

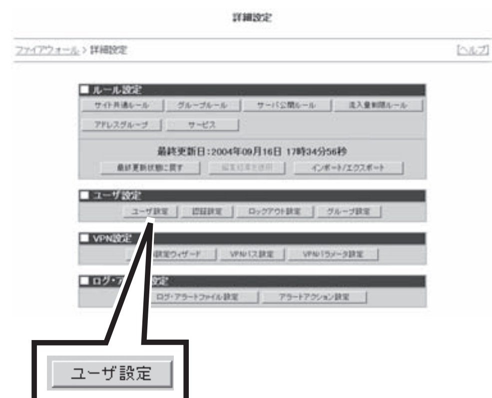
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

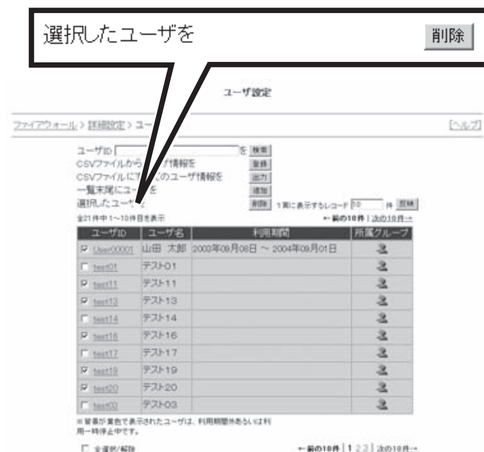
3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

   ユーザ情報一覧画面が表示されます。



詳細設定メニュー画面

4. 削除したいユーザのチェックボックスにチェックをつけ、「選択したユーザを『削除』」をクリックする。



ユーザ情報一覧画面

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。



[キャンセル]をクリックすると、削除されずにユーザ情報一覧画面に戻ります。

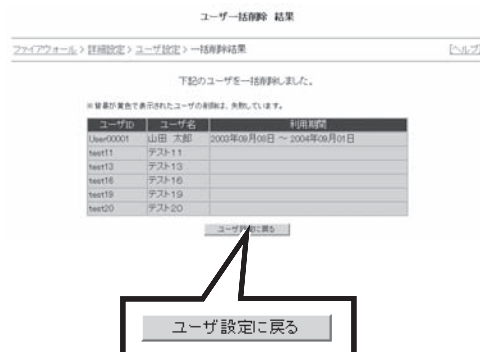
ユーザ情報が削除され、ユーザ一括削除結果画面が表示されます。



背景が黄色のユーザ情報は、削除に失敗したレコードであることを示します。

6. [ユーザ設定に戻る]をクリックする。

ユーザ情報一覧画面に戻ります。このとき、削除したユーザ情報は一覧に表示されません。



ユーザ一括削除結果画面

ユーザ情報の更新

ユーザ情報に変更があった場合、変更のあった項目のみ更新することができます。

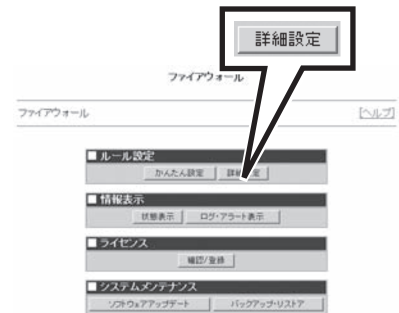
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

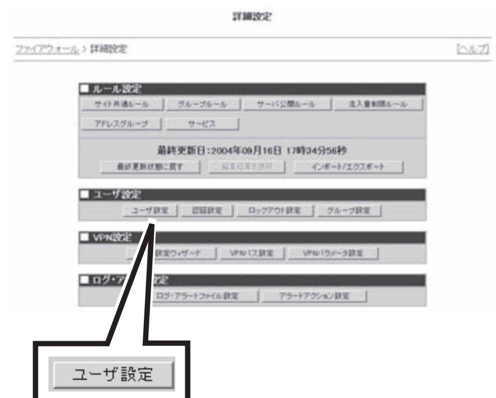
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ユーザ設定]をクリックする。

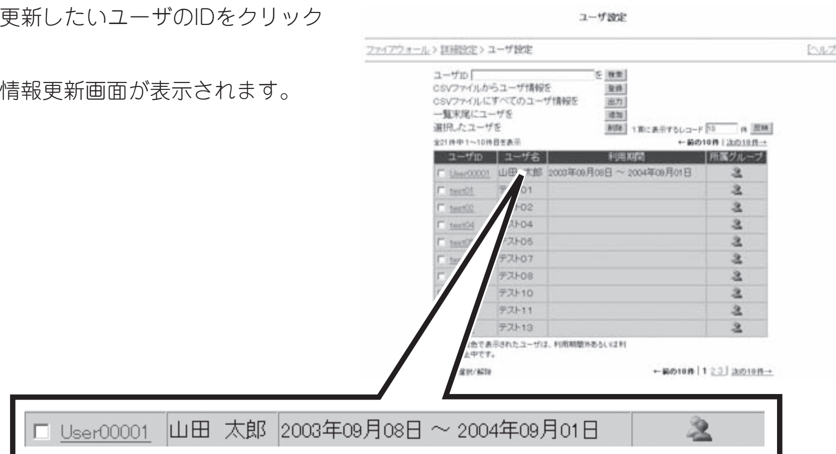
   ユーザ情報一覧画面が表示されます。



詳細設定メニュー画面

4. 情報を更新したいユーザのIDをクリックする。

ユーザ情報更新画面が表示されます。



ユーザ情報一覧画面

5. ユーザ情報更新画面で更新したい項目を入力する。



ユーザ情報更新画面

- ユーザ名
  ユーザを表す名称を入力します。最大で128バイトまでの任意の文字列を受け付けます。ただし、二重引用符(")とカンマ(,)を含めることはできません。
- ユーザID
  変更することはできません。
- パスワード
  ユーザのパスワードを入力します。6バイトから256バイトまでの英数文字列を受け付けます。空白の場合、すでに登録されているパスワードが適用されます。
- 再パスワード
  ユーザのパスワードをもう一度入力します。空白の場合、すでに登録されているパスワードが適用されます。
- 備考
  ユーザに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。
- 利用期間
  ユーザの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、ユーザはログインできません。
- 利用を一時停止する
  運用上の理由などにより、ユーザの利用を一時停止したい場合、このチェックボックスにチェックをつけます。

6. ［更新］をクリックする。

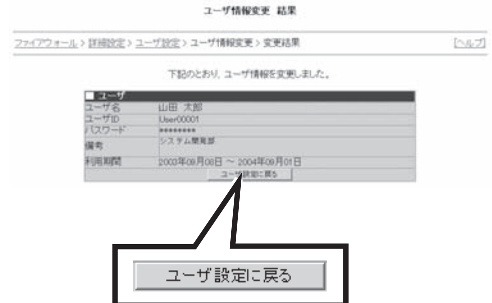
ユーザ情報更新結果画面が表示されます。



ユーザ情報の登録内容が入力規則に違反している場合は、エラー内容を示す画面が表示されます。

7. ［ユーザ設定に戻る］をクリックする。

ユーザ情報一覧画面に戻ります。このとき、更新したユーザ情報が一覧に反映された形で表示されます。



ユーザ情報更新結果画面

ユーザ情報のCSVファイルへの出力

Express5800/SG300が管理しているユーザ情報をCSVファイルに出力することができます。

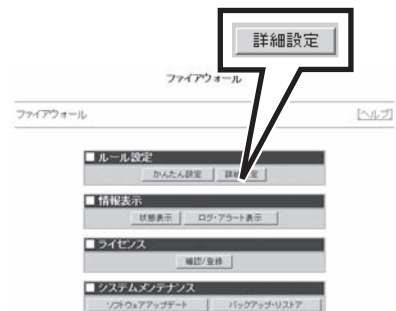
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから［ファイアウォール］をクリックする。

ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から［詳細設定］をクリックする。

詳細設定メニュー画面が表示されます。

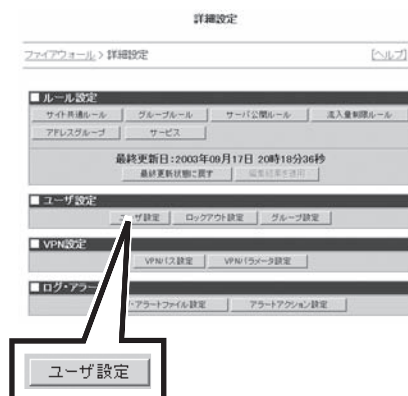


ファイアウォールメニュー画面

ファイアウォール機能の設定方法

3. 詳細設定メニューの「ユーザ設定」から〔ユーザ設定〕をクリックする。

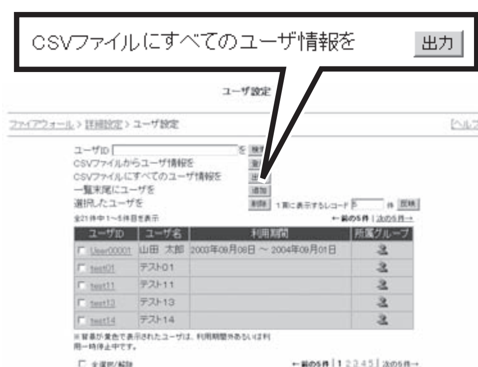
ユーザ情報一覧画面が表示されます。



詳細設定メニュー画面

4. 「CSVファイルにすべてのユーザ情報を『出力』」をクリックする。

ファイル保存先指定画面が表示されます。



ユーザ情報一覧画面

5. ファイル名と保存先を指定し、〔保存〕をクリックする。

管理クライアント上に以下の形式でCSVファイルが保存されます。

カラム	項　目
1	ユーザID
2	認証方式
3	パスワード
4	システム情報
5	システム情報
6	利用一時停止フラグ
7	システム情報
8	利用開始年月日
9	利用停止年月日
10	ユーザ名
11	備考



出力に失敗した場合は、エラー内容を示す画面が表示されます。

認証設定

外部ネットワークから内部ネットワークに存在する端末にアクセスするときや、内部ネットワークから外部ネットワークに存在する端末にアクセスするときは、ファイアウォールとなるExpress5800/SG300を介して通信を行います。このとき、ユーザ認証によりユーザごとに使用する通信を許可することができます。ユーザ認証の利用の設定では、ユーザ認証を利用するかどうかを設定します。



- ユーザの認証は、「ユーザ設定」で登録したユーザID、パスワードにより行います。また、認証を行ったユーザごとに通信の許可を行う場合は、ユーザを「グループ設定」でユーザグループに所属させ、該当ユーザグループの「グループルール」を設定する必要があります。
- 認証設定は、かんたん設定ウィザードからも設定することができます。ここで認証設定を更新すると、かんたん設定ウィザードで設定した認証設定も更新されます。



リモートアクセスVPNを利用する場合は、「ユーザ認証を利用する」に設定してください。認証の受付は「すべてのネットワークから許可する」に設定してください。

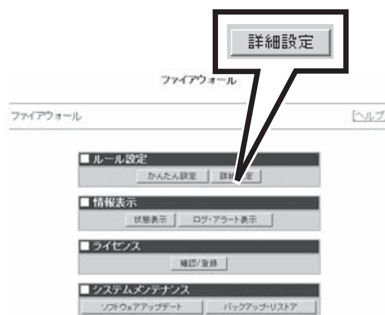
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

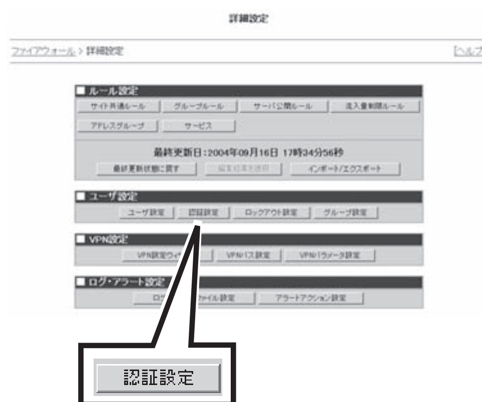
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[認証設定]をクリックする。

   ユーザ認証設定画面が表示されます。



詳細設定メニュー画面

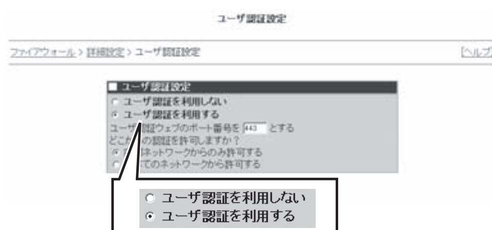
4. ユーザ認証の利用の有無を選択する。

●ユーザ認証を利用しない

ユーザ認証を利用しない場合は、このラジオボタンをクリックし、手順7に進みます。

●ユーザ認証を利用する

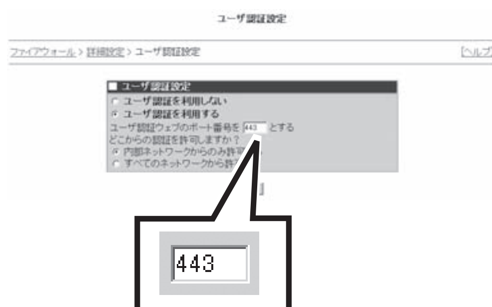
ユーザ認証を利用する場合は、このラジオボタンをクリックし、手順5に進みます。



ユーザ認証設定画面

5. ユーザ認証ウェブのポート番号を指定する。

デフォルトでは「443」に設定されています。通常変更する必要はありません。



ユーザ認証設定画面

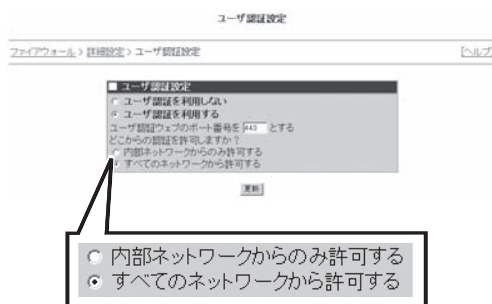
6. ユーザ認証の受付を設定する。

●内部ネットワークからのみ許可する

ユーザ認証のためのアクセスを、内部ネットワークからのみ受付けます。

●すべてのネットワークから許可する

ユーザ認証のためのアクセスを、どこからでも受け付けます。



ユーザ認証の受付画面

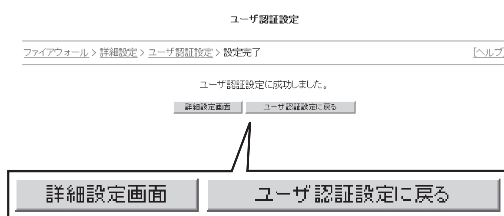
7. ［更新］をクリックする。

ユーザ認証設定完了画面が表示されます。

8. 画面に表示されているいずれかのボタンをクリックする。

［詳細設定画面］をクリックすると詳細設定画面が表示されます。

［ユーザ認証設定に戻る］をクリックすると設定が反映されたユーザ認証設定画面が表示されます。



ユーザ認証設定完了画面

ロックアウト設定

複数回に渡りユーザ認証に失敗したユーザについて、一定期間そのユーザをロックアウトすることができます。



ロックアウトとは、繰り返し認証に失敗すると、一定時間そのユーザ名でログインすることを無条件に禁止し、その間は正しいパスワードを入力してもログインさせない仕組みです。本機能により、パスワードを繰り返し入力することによって、正しいパスワードを特定し、認証を通過しようとする攻撃を防ぐことが可能です。

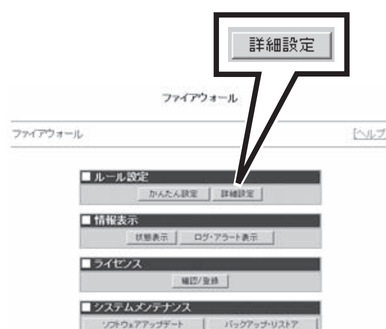
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

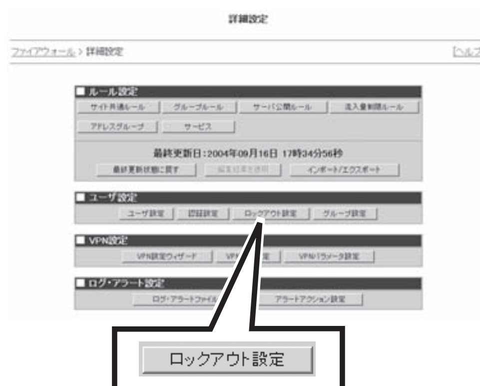
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[ロックアウト設定]をクリックする。

   ロックアウト設定画面が表示されます。



詳細設定メニュー画面

4. 画面に従い認証失敗をカウントする時間(秒)、ロックアウトするまでの回数、ロックアウトされたユーザによるログイン不能な時間(秒)を設定する。



[フォームのデータを元に戻す]をクリックすると、変更前の値に戻ります。

5. [適用]をクリックする。

入力したロックアウト設定の内容でロックアウト機能を適用され、ロックアウト設定完了画面が表示されます。



[ロックアウトの解除]をクリックすると、ロックアウト中の全ユーザのロックアウトを解除します。クリックすると確認画面が表示されるので、ロックアウトを解除する場合は[OK]をクリックします。解除が完了すると、解除完了画面が表示されます。

適用

ロックアウト設定画面

6. [ロックアウト設定に戻る]をクリックする。

ロックアウト設定に戻る

グループ設定

Express5800/SG300を利用したユーザ管理では、グループを作成しユーザをグループ分けして管理することができます。グループ設定では、以下のような操作を行えます。

- グループ情報の確認
  現在登録されているグループ情報を確認することができます。
- グループ情報の追加
  グループ情報を新規に追加します。
- グループ情報の削除
  登録したグループ情報を削除します。
- グループ情報の更新
  登録したグループ情報の内容を変更します。

グループ情報の確認

登録されているグループ情報を確認することができます。

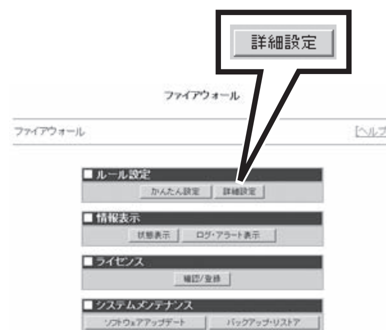
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

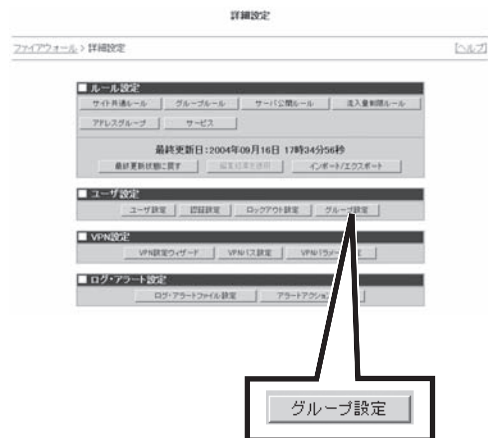
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

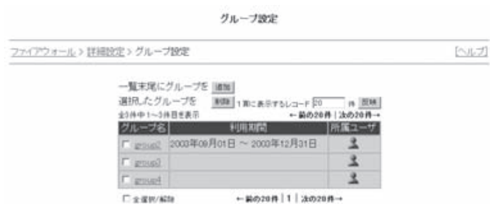
ファイアウォール機能の設定方法

3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。



詳細設定メニュー画面

グループ情報一覧画面が表示されます。表示される内容は以下の通りです。



グループ情報一覧画面

- グループ名
  登録されているグループの名称です。
- 利用期間
  利用可能な期間です。
- 所属ユーザ
  アイコンをクリックするとユーザの情報を確認することができます。



「1頁に表示するレコード」の入力フィールドに件数を入力し、[反映]をクリックすると、その指定した件数でグループ情報を一覧表示します。

グループ情報の追加

グループ情報を新規に作成し、追加することができます。

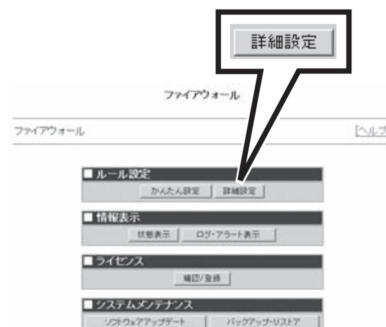
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

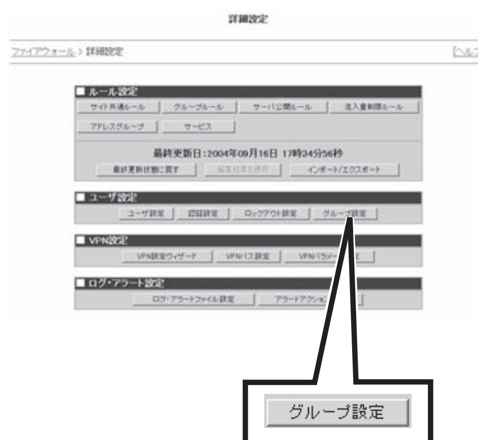
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

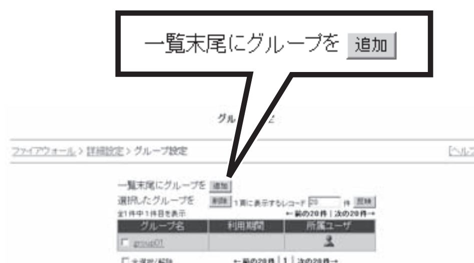
   グループ情報一覧画面が表示されます。



詳細設定メニュー画面

4. 「一覧末尾にグループを『追加』」をクリックする。

   グループ情報追加画面が表示されます。



グループ情報一覧画面

ファイアウォール機能の設定方法

5. グループ情報追加画面に表示される各項目を入力する。

- グループ名(必須項目)
  追加するグループを表す名称を入力します。最大で256バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。既に同じ名前のグループ名がある場合には登録に失敗します。

グループ情報追加画面

- 利用期間
  追加するグループの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、追加するグループに対応したグループルールの適用はされません。
- 備考
  追加するグループに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

6. [登録]をクリックする。

グループ情報追加結果画面が表示されます。

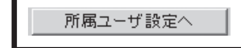
グループ情報追加画面

7. 所属ユーザを設定する場合は、[所属ユーザ設定へ]をクリックする。所属ユーザ設定画面が表示されるので、ユーザIDから所属させるユーザのチェックボックスをチェックし、[更新]をクリックする。

所属ユーザ設定結果画面が表示されます。



グループに所属するユーザを設定するには、あらかじめ「ユーザ設定」をする必要があります。「ユーザ設定」については、213ページを参照してください。



グループ情報追加結果画面

8. 所属ユーザ設定結果画面の[グループ設定に戻る]をクリックする。

   グループ情報一覧画面に戻ります。このとき、新しく登録されたグループ情報が一覧に反映された形で表示されます。



所属ユーザ設定結果画面

グループ情報の削除

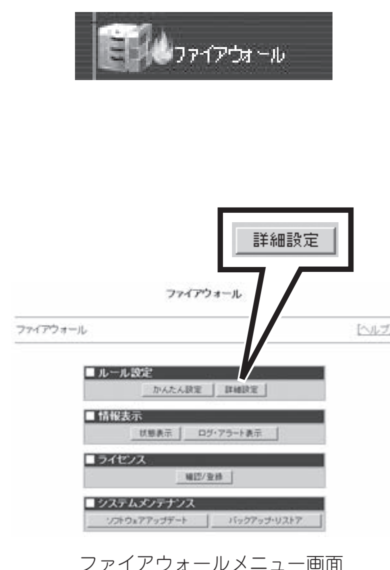
不要になったグループを削除することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

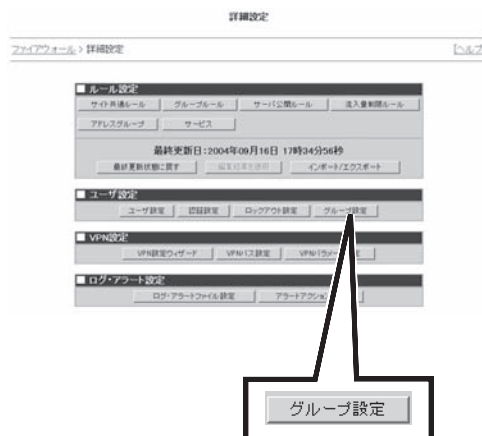
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

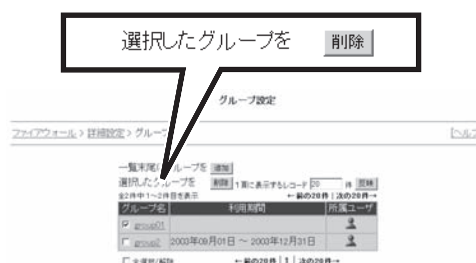
3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

グループ情報一覧画面が表示されます。



詳細設定メニュー画面

4. 削除したいグループ名のチェックボックスにチェックをつけ、「選択したグループを『削除』」をクリックする。



グループ情報一覧画面

5. 別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックする。



[キャンセル]をクリックすると、削除されずにグループ情報一覧画面に戻ります。

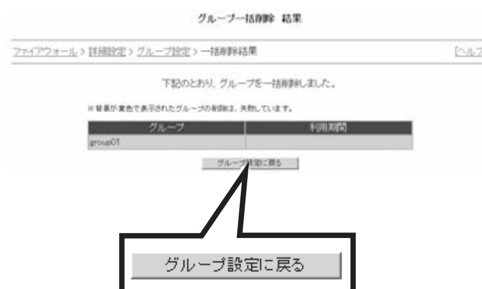
グループ情報が削除され、グループ一括削除結果画面が表示されます。



背景が黄色のグループ情報は、削除に失敗したレコードであることを示します。

6. [グループ設定に戻る]をクリックする。

グループ情報一覧画面に戻ります。このとき、削除したグループ情報は一覧に表示されません。



グループ一括削除結果画面

グループ情報の更新

グループ情報に変更があった場合、変更のあった項目のみ更新することができます。

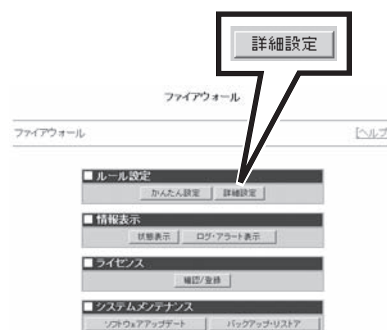
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

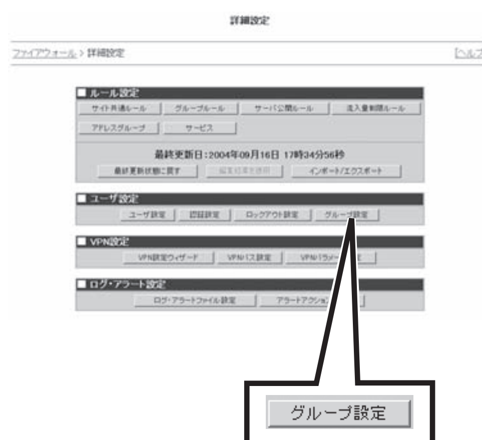
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ユーザ設定」から[グループ設定]をクリックする。

   グループ情報一覧画面が表示されます。



詳細設定メニュー画面

4. 情報を更新したいグループ名をクリックする。

   グループ情報更新画面が表示されます。



グループ情報一覧画面

5. グループ情報更新画面で更新したい項目を入力する。

- グループ名
  変更することはできません。
- 利用期間
  グループの利用期間を限定するか、無制限にするかを選択します。利用期間外のときには、グループに対応したグループルールの適用はされません。

グループ情報更新画面

- 備考
  グループに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

6. ［更新］をクリックする。

グループ情報更新結果画面が表示されます。

7. ［グループ設定に戻る］をクリックする。

グループ情報一覧画面に戻ります。このとき、更新したグループ情報が一覧に反映された形で表示されます。

8. 所属ユーザを更新する場合は、グループ情報一覧画面に表示される所属ユーザ情報のアイコンをクリックする。

所属ユーザ設定画面が表示されます。



グループ情報一覧画面

9. ユーザIDから所属させるユーザのチェックボックスをチェックし、[更新]をクリックする。

所属ユーザ設定結果画面が表示されます。



所属ユーザ選択画面

10. [グループ設定に戻る]をクリックする。

グループ情報一覧画面に戻ります。このとき、変更したグループ情報が一覧に反映された形で表示されます。



所属ユーザ設定結果画面

VPN設定

Express5800/SG300はIPSecを利用したVPN通信を行うことができます。VPNパスの管理では、VPN通信を行うパスの設定や暗号通信方式の設定を行うことができます。ただし、VPNパスの中を通る通信が無条件に許可されることはないため、ここで定義したVPNパスの中を通る個々の通信については、別途フィルタリング設定が必要です。フィルタリング設定については、121ページの「サイト共通ルール」を参照してください。また、Express5800/SG300でVPN通信を行わず、他のVPN機器同士のVPN通信を通過させる場合は、「VPN設定」の対象となりません。この場合、「サイト共通ルール」で通信種別IPSecについて、フィルタリング設定を行う必要があります。
VPNパスの管理では、以下の項目の設定・管理を行います。

VPN設定ウィザード .... ウィザード形式でVPN設定を行うことができます。

VPNパス設定 .... VPNのパスを環境にあわせて自由に設定することができます。

VPNパラメータの設定 .... 同時に利用できるVPNトンネル数、トランスポート数の設定を行うことができます。



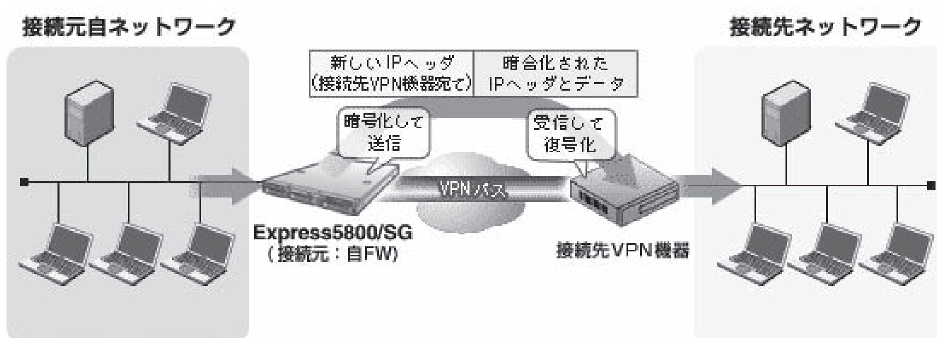
- **VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があると、VPN通信は行えません。**
- **VPN接続時に、停電などによりExpress5800/SG300の電源がOFFになると、相手側VPN機器にセキュリティアソシエーション(SA)が残るため、その残ったSAの有効時間が切れるまではVPN接続ができなくなります。**
- **Express5800/SG300自身がIPSecを使用せず、他サーバ間のIPSec通信の間に入る場合、ここでのVPN設定は不要です。ただし、サイト共通ルールで、サーバ間のIPSec通信を許可しておく必要があります。なお、このとき、かんたん設定で「アドレス変換(NAT/NAPT)を行う」設定をしていると、問題が起こることがあります(サーバ間のIPSecでAHを使用している場合)。**
- **Express5800/SG300でIPSecを使用し、接続先との経路上にファイアウォールが存在する場合、そのファイアウォールにおいて、IKEで使用するUDP 500番ポート、AH(プロトコル番号51)、ESP(プロトコル番号50)を通過できるように設定する必要があります。また、上記条件のもと、かんたん設定で「アドレス変換(NAT/NAPT)を行う」を設定し、AHを使用するように設定した場合、問題が起こることがあります(これはIPSecの仕様による制限です)。**

VPN設定ウィザード

複雑なVPN設定をウィザード形式で簡単に設定することができます。
VPNの接続方式としては、LANとLANをVPN接続するLAN間接続VPN(Gateway to Gateway VPN)と、リモート端末からVPN機器にアクセスして公開されたサーバにアクセスするリモートアクセスVPN(Host to Gateway VPN)があります。

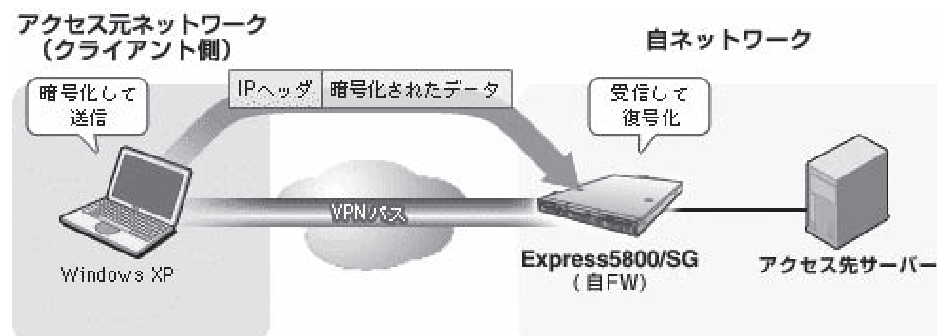
● LAN間接続VPN(Gateway to Gateway VPN):トンネルモード

LAN間接続VPN(Gateway to Gateway VPN)では、自ネットワーク側LANのゲートウェイとなるExpress5800/SG300と通信相手側LANのGatewayとなるVPN通信機器間で暗号通信を行い、装置間にあたかも仮想的なトンネルがあるかのように接続を行います。この方式では、IPヘッダを含めたIPパケット全体を暗号化し、暗号化処理を行う装置のIPアドレスを宛先として通信します。



● リモートアクセスVPN(Host to Gateway VPN):トランスポートモード

リモートアクセスVPN(Host to Gateway VPN)では、通信を行う端末間で暗号通信を行います。IPヘッダの暗号化は行いません。





VPN設定ウィザードでは、プリシェアードシークレットを利用した自動鍵交換方式のVPN通信の設定ができます。
事前共有鍵交換方式のVPN通信の設定は、「VPNパス設定」で追加することができます。

LAN間接続

LAN間接続VPNとは、2つのLANとLANのGatewayとなるVPN機器(Express5800/SG300等)の間にVPNパスを設定し、暗号化通信を行う方式です。
VPN設定ウィザードで設定したLAN間接続VPNは、自動鍵交換方式のトンネルモードとなります。



- **VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があると、VPN通信は行えません。**
- **VPN接続時に、停電などによりSG300の電源がOFFになると、相手側VPN機器にセキュリティアソシエーション(SA)が残るため、その残ったSAの有効時間が切れるまではVPN接続ができなくなります。**

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

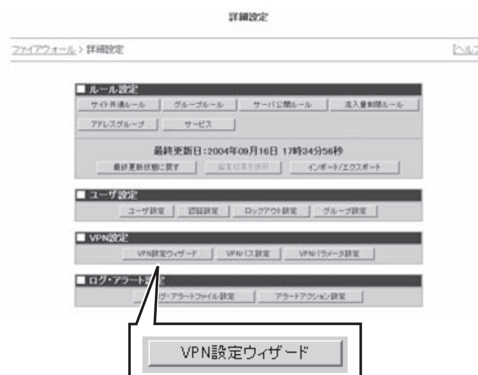
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPN設定ウィザード]をクリックする。

   VPN設定ウィザードが表示されます。



詳細設定メニュー画面

4. 「LAN間接続VPN」をクリックする。



VPN設定ウィザード画面

5. ［次へ］をクリックする。

LAN間接続VPN設定画面が表示され、LAN間接続VPNの設定に進みます。

6. LAN間接続VPNを設定する。

●接続先VPN機器のIPアドレス

接続する先のVPN機器が外部に公開しているIPアドレスを設定します。

●名称

LAN間接続VPNを識別する任意の文字列を指定します。
名称は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

●備考

LAN間接続VPNに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。



VPN設定ウィザード画面

7. ［次へ］をクリックする。

許可パス設定画面が表示され、許可パスの設定に進みます。

8. 許可パスを設定する。

●自ネットワークアドレス

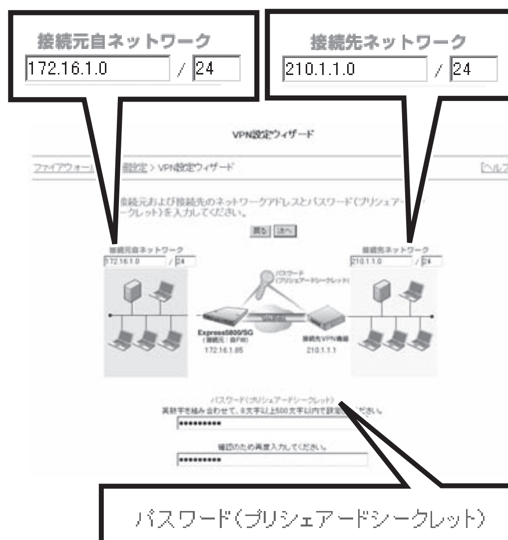
自分側のネットワークアドレスを設定します。

●接続先ネットワークアドレス

LAN間接続VPNで接続する先のネットワークのアドレスを設定します。

●プリシェアードシークレット

あらかじめ、接続先と決めておいたプリシェアードシークレットを設定します。プリシェアードシークレットはVPNを使った暗号通信を実現するために必要なパスワードのようなものです。



VPN設定ウィザード画面



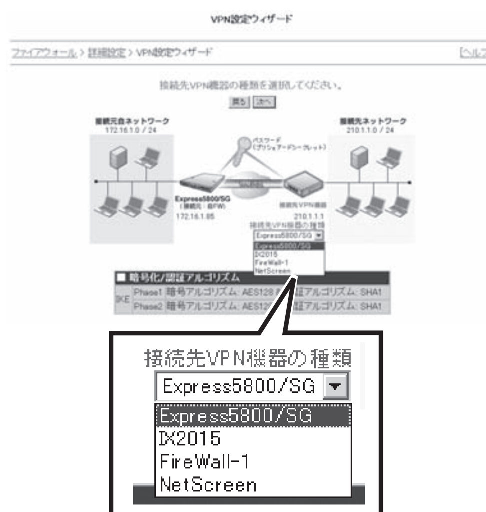
プリシェアードシークレットには必ず英数字を組み合わせた8文字以上500文字以内の文字列を設定してください。

9. [次へ]をクリックする。

暗号化/認証アルゴリズム設定画面が表示され、接続先VPN機器の設定に進みます。

10. プルダウンメニューから「接続先VPN機器の種類」を選択する。

接続先VPN機器は、「Express5800/SG」、「IX2015」「Firewall-1」、「NetScreen」から選択することができます。



VPN設定ウィザード画面

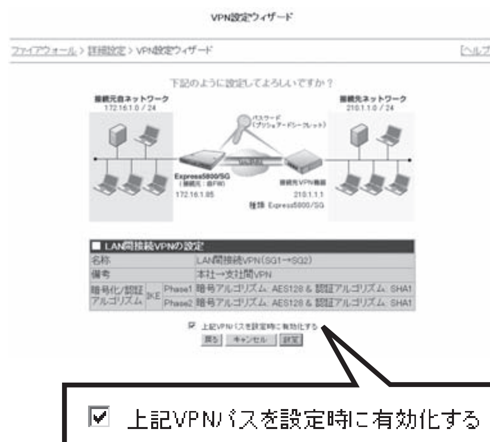


- 接続先VPN機器を選択すると、自動的に適した暗号化アルゴリズムと認証アルゴリズムが設定されます。
- 表示される機器以外のVPN機器をご利用の場合は、「VPNパス設定」で暗号化アルゴリズムと認証アルゴリズムを変更することができます。

11. [次へ]をクリックする。

設定内容確認画面が表示されます。

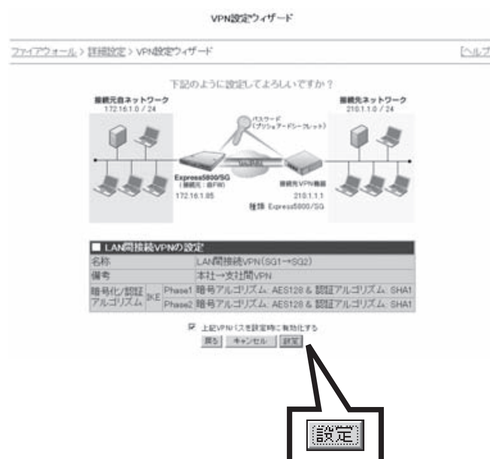
12. 設定内容を確認する。設定した内容をすぐに適用するには、[上記VPNパスを設定時に有効にする]のチェックボックスにチェックする。



VPN設定ウィザード画面

13. 問題がなければ[設定]をクリックする。

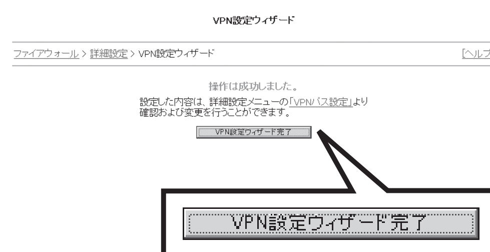
設定が誤っている場合は、[戻る]で設定画面に戻ることができるので、設定をやり直してください。[キャンセル]をクリックすると、これまでの設定内容が破棄されます。



VPN設定ウィザード画面

[設定]をクリックし、内容が正常に設定された場合は、結果画面が表示されます。

[VPN設定ウィザード完了]をクリックすると、詳細設定メニュー画面に戻ります。



VPN設定ウィザード画面



ここで設定したVPNパスの内容は、[VPNパス設定]から、変更することができます。

リモートアクセスVPN

リモートアクセスVPNとは、ネットワークから離れた場所にある端末からネットワーク内のExpress5800/SG300の間にVPNパスを設定し、暗号化通信を行う方式です。このとき、サーバへのアクセス設定を行うことで、指定したサーバへのユーザからのアクセスを受け付けることができます。
リモートアクセスVPNを構築することにより、自宅や出張先からインターネット経由で企業内ネットワークへ安全にアクセスすることが可能になります。
VPN設定ウィザードで設定したリモートアクセスVPNは、自動鍵交換方式のトランスポートモードとなります。



- **リモートアクセスVPN環境を構築するには、ユーザ認証が必須となります。そのため、VPN設定前の事前準備として、「かんたん設定」のユーザ認証の利用の設定または詳細設定メニューの「認証設定」よりユーザ認証が利用できるように設定しておく必要があります。「ユーザ認証」については、227ページを参照してください。**
- **VPN通信を行うネットワークの途中にアドレス変換(NAT/NAPT)を行う機器があると、VPN通信は行えません。**
- **VPN接続時に、停電などによりExpress5800/SG300の電源がOFFになると、相手側端末にセキュリティアソシエーション(SA)が残るため、その残ったSAの有効時間が切れるまではVPN接続ができなくなります。**

リモートアクセスVPNの設定

リモートアクセスVPNでは、クライアントアドレス(リモートからVPN通信で内部ネットワークにアクセスする端末のIPアドレス)を任意とするVPNパス(自動鍵交換：トランスポートモード)を1つ設定します。
複数のサーバのリモートアクセスを許可するには、そのVPNパス設定を利用してVPN設定ウィザードから公開するサーバのIPアドレスを指定します。公開するサーバごとに、グループが作成されます。
VPN設定ウィザードを利用した2回目以降の設定は、250ページの「アクセス先サーバが2台以上ある場合の設定について」を参照してください。

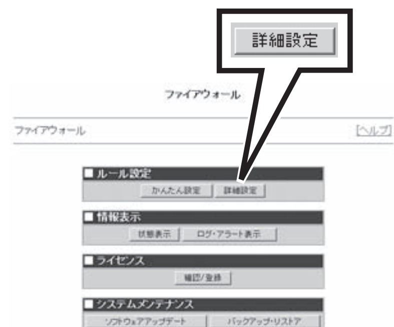
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

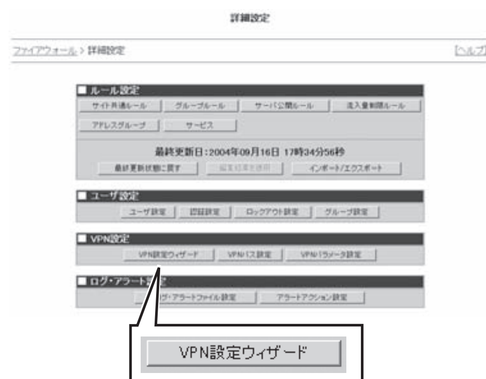
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

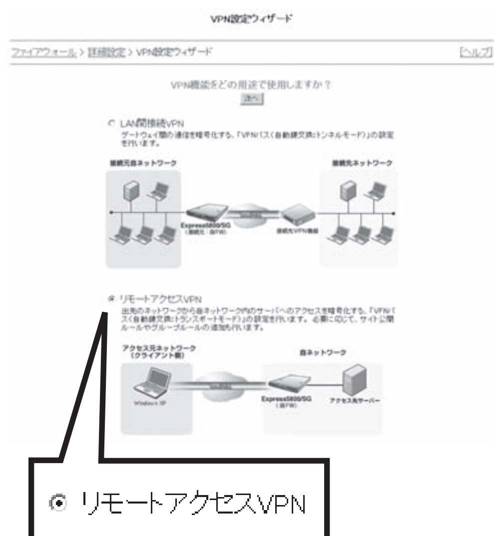
3. 詳細設定メニューの「VPN設定」から[VPN設定ウィザード]をクリックする。

VPN設定ウィザードが表示されます。



詳細設定メニュー画面

4. 「リモートアクセスVPN」をクリックする。



VPN設定ウィザード画面

5. [次へ]をクリックする。

リモートアクセスVPN設定画面が表示され、リモートアクセスVPNの設定に進みます。

6. リモートアクセスVPNを設定する。

●名称

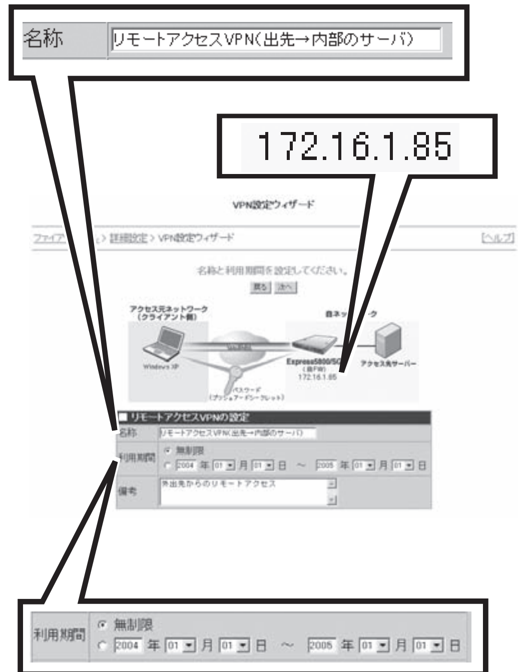
リモートアクセスVPNを識別する任意の文字列を指定します。
名称は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。

●利用期間

リモートアクセスVPNの利用期間を制限しない場合は「無制限」をクリックします。
期間を制限する場合は、プルダウンメニューを使って利用期間を指定します。

●備考

リモートアクセスVPNに関する備考を入力します。最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(“)およびカンマ(,)を含めることはできません。入力は任意です。



VPN設定ウィザード画面



名称には、既に設定した名称と同様の名称は設定することができません。



「このVPNパスを利用するユーザのグループ」として、ここで設定した名称で新しくグループとグループルールが追加されます。グループへのユーザ登録は手順14で行うことができます。

7. [次へ]をクリックする。

プリシェアードシークレット設定画面が表示され、プリシェアードシークレットの設定に進みます。

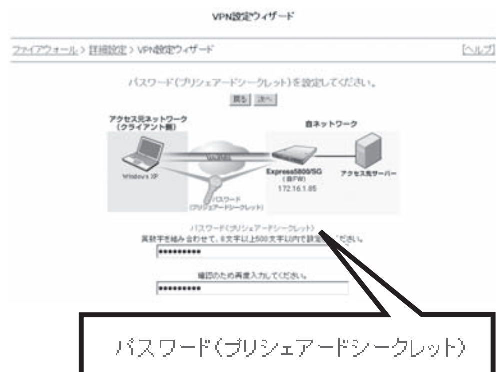
8. プリシェアードシークレットを設定する。

●プリシェアードシークレット

あらかじめ、接続先と決めておいたプリシェアードシークレットを設定します。プリシェアードシークレットはVPNを使った暗号通信を実現するために必要なパスワードのようなものです。



プリシェアードシークレットは必ず英数字を組み合わせた8文字以上500文字以内の文字列を設定してください。



VPN設定ウィザード画面

9. ［次へ］をクリックする。

アクセス先サーバ設定画面が表示され、リモート端末からVPN接続でアクセスするサーバの設定に進みます。

10. リモートからアクセスを許可するサーバを設定する。

●アクセス先サーバの内部IPアドレス

リモートからアクセスを許可するサーバの内部IPアドレスを設定します。

●アドレス変換の設定

アドレス変換時のポート番号を設定します。外部ネットワークに公開するポート番号と対応する内部ポート番号を設定します。TCPとUDPをラジオボタンで指定することができます。



公開するIPアドレスやポート番号の変換については、「サーバ公開ルール」の設定内容に影響します。

設定の途中で設定済みのサーバ公開ルールを確認したい場合は、画面下の説明文中の「既存の設定を確認する」をクリックしてください。



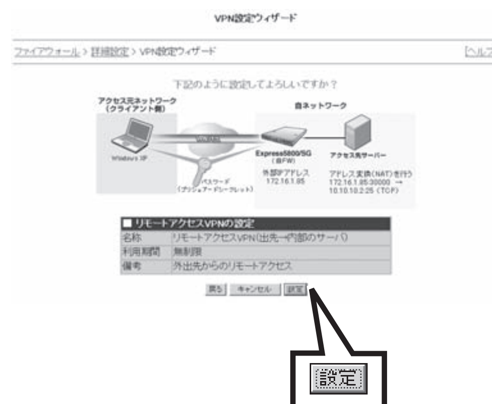
VPN設定ウィザード画面

11. ［次へ］をクリックする。

設定内容確認画面が表示されます。

12. 設定内容を確認し、問題がなければ［設定］をクリックする。

設定が誤っている場合は、［戻る］で設定画面に戻ることができるので、設定をやり直してください。［キャンセル］をクリックすると、これまでの設定内容が破棄されます。



VPN設定ウィザード画面

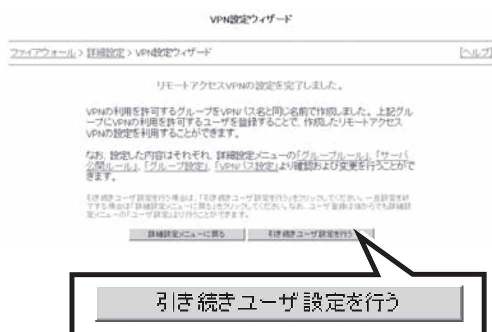
［設定］をクリックし、内容が正常に設定された場合は、結果画面が表示されます。



ここで設定した内容は、「グループルール」、「サーバ公開ルール」、「グループ設定」、「VPNパス設定」に影響します。また、各設定画面から変更することができます。

13. リモートからアクセスするユーザを設定する場合は、［引き続きユーザ設定を行う］をクリックする。

ユーザ設定画面が表示されます。ユーザ設定については、213ページの「ユーザ設定」を参照してください。



VPN設定ウィザード画面

アクセス先サーバが2台以上ある場合の設定について

複数のサーバへのリモートアクセスを許可する場合は、VPN設定ウィザードから同じように設定します。ただし、2回目以降は、VPNパス（自動鍵交換：トランスポートモード）の設定は完了しているため、プリシェアードシークレットは設定する必要がありません。「名称」、「利用期間」、「アクセス先サーバのIPアドレス」、および「NAT設定」のみを設定します。プリシェアードシークレットを変更すると、その他のリモートアクセスVPNのプリシェアードシークレットも変更されますので注意してください。
なお、「名称」はすでに設定した名称と同じ名称は設定できません。同じものがある場合は、設定確認時に変更画面が表示されます。自動的に、設定した名称の末尾に「其の2」、「其の3」と番号が付与されますが、任意の文字列に変更することもできます。
ここでは、2回目以降のリモートアクセスVPNの設定について説明します。VPN設定ウィザードの表示以降から説明します。

1. VPN設定ウィザードで「リモートアクセスVPN」をクリックする。

2. ［次へ］をクリックする。

   VPNパス設定画面が表示され、VPNパスの設定に進みます。

3. VPNパスを設定する。

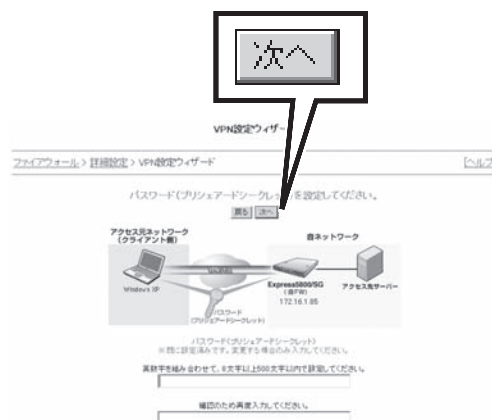
   ●名称
   ●利用期間
   ●備考

4. ［次へ］をクリックする。

   プリシェアードシークレット設定画面が表示され、プリシェアードシークレットの設定に進みます。

5. すでに設定しているVPNパス(自動鍵交換：トランスポートモード)と同様のプリシェアードシークレットを利用する場合は、入力せずに[次へ]をクリックする。変更する場合は、プリシェアードシークレットを入力する。

   アクセス先サーバ設定画面が表示され、リモート端末からVPN接続でアクセスするサーバの設定に進みます。



VPN設定ウィザード画面

6. リモートからアクセスを許可するサーバを設定する。

   ●アクセス先サーバの内部IPアドレス

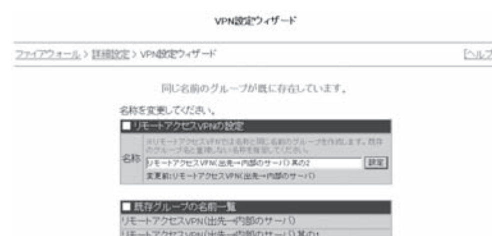
   ●アドレス変換の設定

7. [次へ]をクリックする。

   設定内容確認画面が表示されます。

8. 設定内容を確認し、問題がなければ[設定]をクリックする。

   「名称」がすでに設定した「名称」と重なっている場合は、名称変更画面が表示されます。自動的に設定した名称の末尾に「其の2」、「其の3」と番号が付与されますが、任意の文字列に変更することもできます。
   手順5でプリシェアードシークレットを入力した場合は、VPNパスの上書き確認画面が表示されます。



9. プリシェアードシークレットを上書きしてもよければ[はい]をクリックする。
   プリシェアードシークレットを上書きしない場合は、[パスワードを変更しないで設定]をクリックする。

10. 設定完了画面が表示される。リモートからアクセスするユーザを設定する場合は、[引き続きユーザ設定を行う]をクリックする。

    ユーザ設定画面が表示されます。ユーザ設定については、213ページの「ユーザ設定」を参照してください。

VPNパス設定

VPNパス設定では、VPN設定ウィザードで設定したVPNパスを変更したり、新たなVPNパスを追加したりすることができます。
VPNパス設定では、以下の項目を設定／管理します。

- VPNパスの確認
- VPNパスの追加（共有鍵交換）
- VPNパスの追加（自動鍵交換：トンネルモード）
- VPNパスの追加（自動鍵交換：トランスポートモード）
- VPNパスの削除
- VPNパスの更新

VPNパス確認

すでに設定したVPNパスはVPN情報一覧画面から確認することができます。

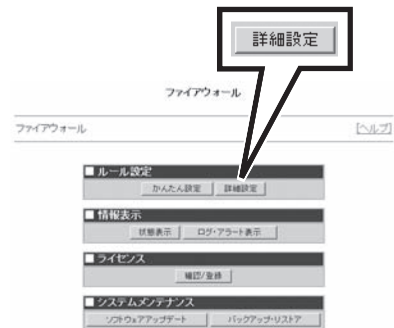
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

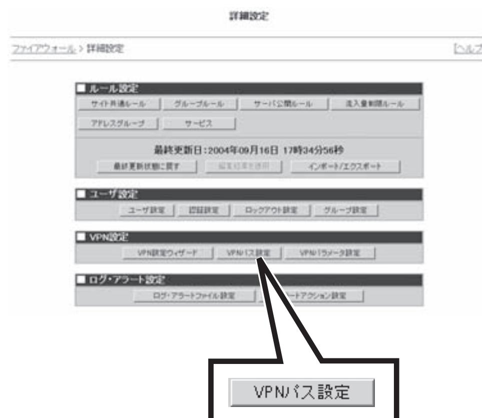
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

VPNパス設定画面が表示されます。表示される内容は以下の通りです。



詳細設定メニュー画面

項　目		説　明
パス番号		VPNパスの番号です。
VPNパス	接続先IPアドレス	VPN通信を行う相手のIPアドレスです。
	自IPアドレス	Express5800/SG300の外部ネットワークに接続したインタフェースに割り当てられたIPアドレスです。
許可パス	接続組み合わせ	VPN通信を行う相手先と自ネットワークの組み合わせです。 自動鍵交換方式のトランスポートモードでは表示されません。
モード		VPN通信を行うモードです。
鍵交換方式		鍵の交換方式です。



VPNパス設定画面



「1頁に表示するレコード」の入力フィールドに件数を入力し、[反映]をクリックすると、その指定した件数でVPNパスを一覧表示します。

VPNパスの追加(共有鍵交換)

必要に応じてVPNパスを追加することができます。ここでは、共有鍵交換方式を利用したVPNパスの設定について説明します。

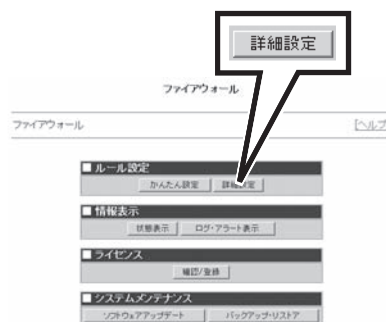
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

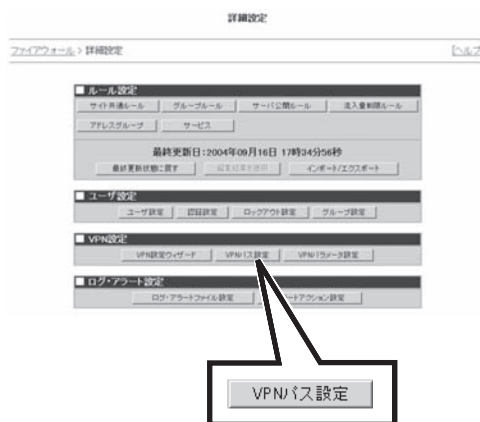
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

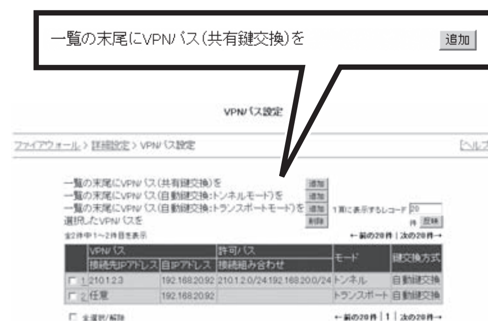
   VPNパス設定画面が表示されます。



詳細設定メニュー画面

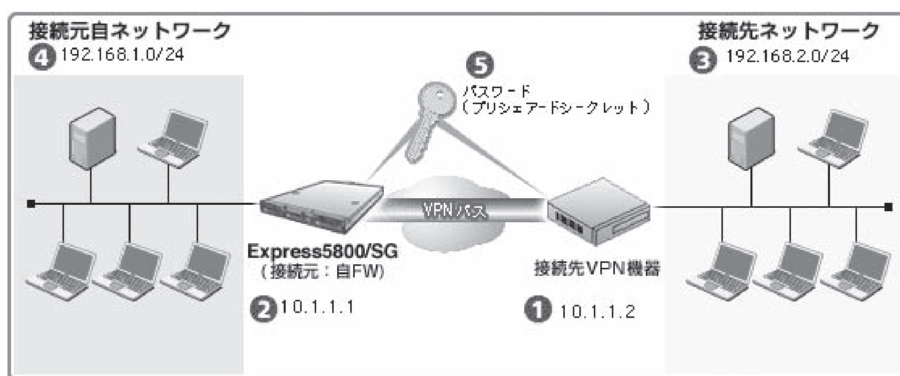
4. 「一覧の末尾にVPNパス(共有鍵交換)を『追加』」をクリックする。

VPNパス(共有鍵交換)画面が表示されます。



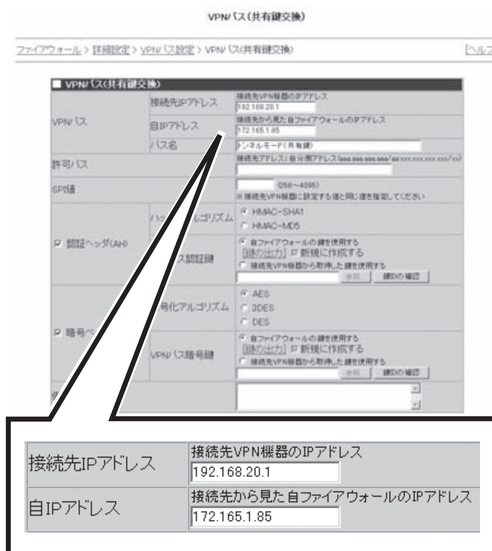
VPNパス設定画面

以降の各項目の設定手順では、VPN通信の概念を理解しやすくするために以下の図を用いて説明します。



5. VPNパスを設定する。

- 接続先IPアドレス
  VPNパスをはる接続先VPN機器が外部に公開しているIPアドレスを入力します(VPNパスの概念図の①)。
- 自IPアドレス
  VPNパスをはる接続先から参照することができる、Express5800/SG300の外部ネットワークにつなげたインタフェースのIPアドレスを入力します(VPNパスの概念図の②)。
- パス名
  VPNパスを識別する任意の文字列を指定します。VPNパス名は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。



VPNパス(共有鍵交換)画面

6. 許可パスを入力する。

VPNパスをはる接続先アドレス（VPNパスの概念図の③）と自分側のアドレス（VPNパスの概念図の④）との組みを入力します。「接続先IPアドレス/ネットマスク:自分側IPアドレス/ネットマスク」のように、ネットマスクを含めた形で指定します。



IPアドレスだけを指定したい場合にはネットマスクを32としてください。

許可パス	接続先アドレス：自分側アドレス(aaa.aaa.aaa.aaa/aa:xxx.xxx.xxx.xxx/xx) 192.168.20.0/24:172.165.1.0/24

VPNパス（共有鍵交換）画面

7. SPI値を入力する。



SPIとはトンネルを一意に特定するIDです。VPNによる暗号化通信を行う接続先との間で取り決めたSPI値を入力します。値の有効範囲は、256から4095までです。

SPI値	887 (256～4095) ※接続先VPN機器に設定する値と同じ値を指定してください

VPNパス（共有鍵交換）画面

8. 認証ヘッダ(AH)を利用する場合、チェックボックスにチェックし、ハッシュアルゴリズムとVPNパス認証鍵の設定を行う。

☑ 認証ヘッダ(AH)	ハッシュアルゴリズム	◉ HMAC-SHA1 ○ HMAC-MD5
	VPNパス認証鍵	◉ 自ファイアウォールの鍵を使用する [鍵の出力] ☑ 新規に作成する ○ 接続先VPN機器から取得した鍵を使用する [参照...] [鍵IDの確認]

VPNパス(共有鍵交換)画面

ヒント

AHはIPヘッダを含めたパケットの改ざん検知を行います。AHはハッシュアルゴリズムを使って送信データとVPNパス認証鍵から認証データを生成し、その認証データを送信データに付与して一緒に送ります。通信相手はデータを受信したとき、同様にハッシュアルゴリズムを使ってデータと認証鍵から認証データを生成し、送られてきた認証データと比較します。通信の途中で第三者がパケットの内容を改ざんした場合は、送信された認証データと受信者の生成した認証データが異なるため、改ざんの有無を検出することができます。

- ハッシュアルゴリズム
  HMAC-SHA1とHMAC-MD5から選択します。あらかじめ通信相手とアルゴリズムを決めておき、通信相手と同様のものを設定します。
- VPNパス認証鍵
  VPNパスの認証に使用する共有鍵を指定します(VPNパスの概念図の⑤)。
  共有鍵は自ファイアウォールと接続先VPN機器で同一の鍵を共有する必要があるため、どちらか一方のノードで鍵を生成し、生成した鍵データをもう一方のノードに転送して利用します。
  - 自ファイアウォールの鍵を使用する
    Express5800/SG300で作成した鍵を使用するときに選択し、[鍵の出力]をクリックして鍵データをファイルに出力します。鍵を新規に作る、または作り直す場合は、「新規に作成する」チェックボックスにチェックをしてから[鍵の出力]をクリックしてください。そのファイルを接続先VPN機器に渡して、VPNパス認証鍵として設定してください。
  - 接続先VPN機器から取得した鍵を使用する
    接続先のVPN機器で作成した鍵を使用するときに選択します。テキストボックスに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックしてファイルを選択してください。
    鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウで表示します。

チェック

読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

9. 暗号化ペイロード(ESP)を利用する場合、チェックボックスにチェックし、暗号化アルゴリズムとVPNパス暗号鍵の設定を行う。


ヒント

ESPではVPNパス暗号鍵と暗号化アルゴリズムを使ってパケットを暗号化することで、通信の機密性を保証します。

☑ 暗号ペイロード(ESP)	暗号化アルゴリズム	◉ AES ○ 3DES ○ DES
	VPNパス暗号鍵	◉ 自ファイアウォールの鍵を使用する [鍵の出力] ☑ 新規に作成する ○ 接続先VPN機器から取得した鍵を使用する [参照...] [鍵IDの確認]

VPNパス(共有鍵交換)画面

- 暗号化アルゴリズム
  暗号化アルゴリズムを、AES、3DES、DESから選択します。あらかじめ通信相手とアルゴリズムを決めておき、通信相手と同様のものを設定します。
- VPNパス暗号鍵
  暗号通信に使用する共有鍵を指定します(VPNパスの概念図の⑤)。
  自ファイアウォールと接続先VPN機器とで1つの鍵を共有する必要があります。したがって、どちらか一方で鍵を生成したらもう一方に同一の鍵データを渡し、渡された方は鍵データを読み込みます。
  - 自ファイアウォールの鍵を使用する
    Express5800/SG300で作成した鍵を使用するときに選択し、[鍵の出力]をクリックして暗号鍵をファイルに出力します。鍵を新規に作る、または作り直す場合は、「新規に作成する」チェックボックスにチェックをしてから[鍵の出力]をクリックしてください。そのファイルを接続先VPN機器に渡して、VPNパス暗号鍵として設定してください。
  - 接続先VPN機器から取得した鍵を使用する
    接続先のVPN機器で作成した鍵を使用するときに選択します。入力フィールドに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックしてファイルを選択してください。
    鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウに表示します。


チェック

読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

10. VPNパスに関する備考を入力する。

最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。

11. [適用]をクリックする。

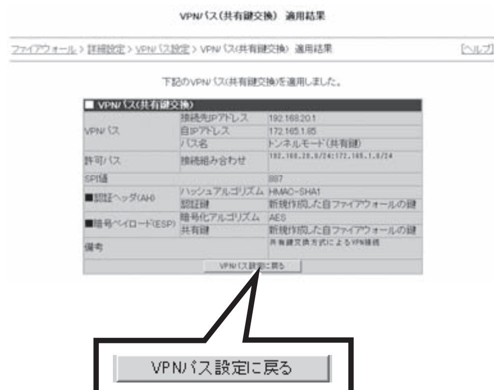
VPNパス(共有鍵交換)適用結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

12. [VPNパス設定に戻る]をクリックする。

追加したVPNパスが反映されたVPNパス設定画面が表示されます。



VPNパス(共有鍵交換)適用結果画面

VPNパスの追加(自動鍵交換：トンネルモード)

必要に応じてVPNパスを追加することができます。ここでは、トンネルモードにおける自動鍵交換方式を利用したVPNパスの設定について説明します。

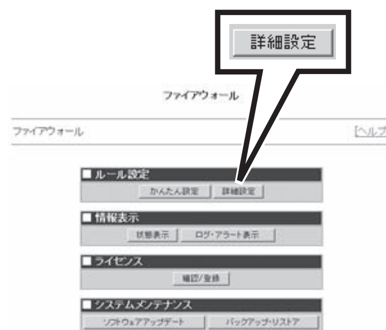
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

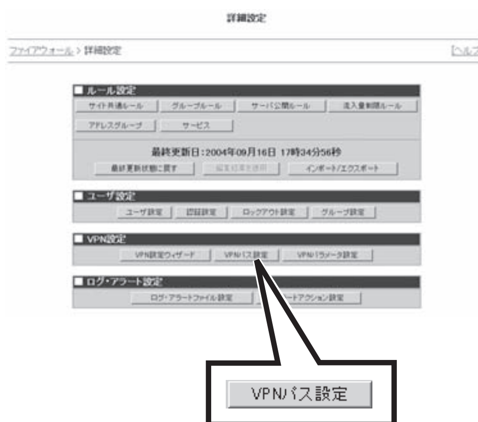
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

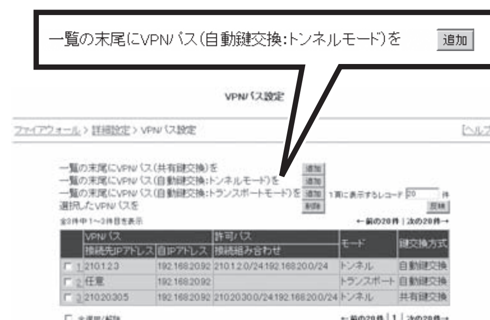
   VPNパス設定画面が表示されます。



詳細設定メニュー画面

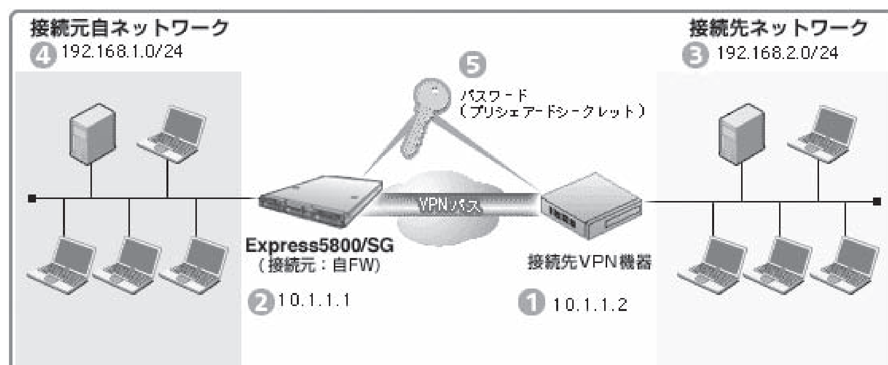
4. 「一覧の末尾にVPNパス(自動鍵交換：トンネルモード)を『追加』」をクリックする。

VPNパス(自動鍵交換：トンネルモード)画面が表示されます。



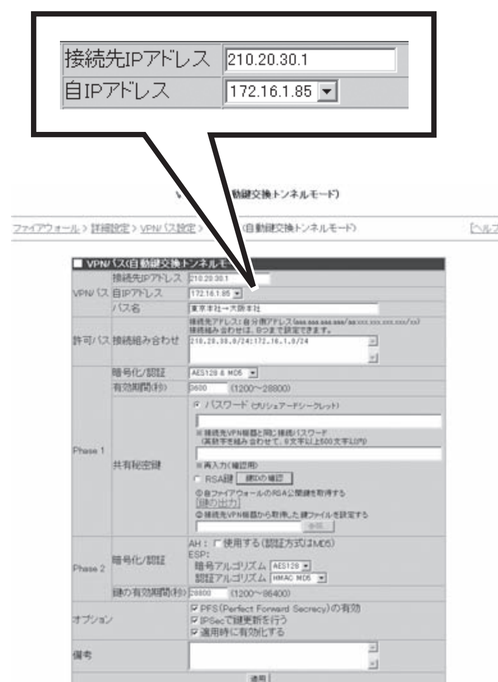
VPNパス設定画面

以降の各項目の設定手順では、VPN通信の概念を理解しやすくするために以下の図を用いて説明します。



5. VPNパスを設定する。

- 接続先IPアドレス
  VPNパスをはる接続先VPN機器が外部に公開しているIPアドレスを入力します(VPNパスの概念図の①)。
- 自IPアドレス
  VPNパスをはる接続先から参照することができる、Express5800/SG300の外部ネットワークにつなげたインタフェースのIPアドレスをプルダウンメニューから選択します(VPNパスの概念図の②)。
- パス名
  VPNパスを識別する任意の文字列を指定します。VPNパス名は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。



VPNパス(自動鍵交換：トンネルモード)画面

6. 許可パスを入力する。

VPNパスをはる接続先アドレス(VPNパスの概念図の③)と自分側のアドレス(VPNパスの概念図の④)との組みを一行に一組ずつ入力します。「接続先IPアドレス/ネットマスク:自分側IPアドレス/ネットマスク」のように、ネットマスクを含めた形で指定します。



IPアドレスだけを指定したい場合にはネットマスクを32としてください。

許可パス	接続組み合わせ	接続先アドレス:自分側アドレス(aaa.aaa.aaa.aaa/aa:xxx.xxx.xxx.xxx/xx) 接続組み合わせは、8つまで設定できます。 210.20.30.0/24:172.16.1.0/24

VPNパス(自動鍵交換:トンネルモード)画面

7. Phase1の「暗号化/認証」、「有効期間」を設定する。



自動鍵交換方式では、最初にIKEを使って通信相手を認証し、暗号化アルゴリズムと暗号鍵を決定します。事前にパスワードまたはRSA鍵を共有していることが条件になります。

IKEでは、まずハッシュアルゴリズムとパスワード(またはRSA鍵)を使って通信相手双方の認証を行います。認証完了後、暗号通信を利用して鍵の元となる乱数データと暗号化アルゴリズムを通知しあい、実際の通信で使用する共通鍵(秘密鍵)を生成します。

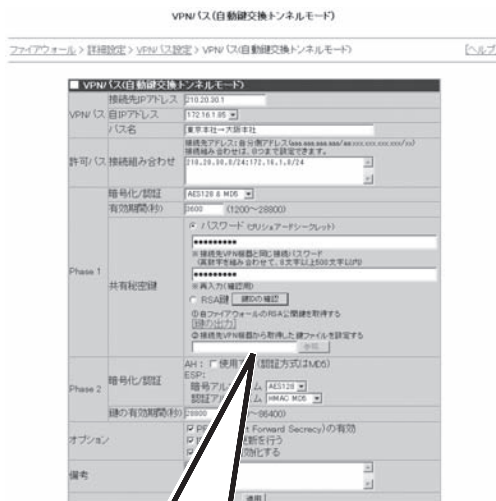
- 暗号化/認証
  IKEの暗号化に利用する暗号化アルゴリズムと認証に利用するハッシュアルゴリズムを設定します。
- 有効期間
  認証完了後の有効期間(秒)を設定します。1200～28800秒まで設定することができます。

暗号化/認証: AES128 & MD5
AES256 & SHA1
AES256
AES128 & MD5
AES128 & SHA1
AES128
3DES & MD5
3DES & SHA1
3DES
DES & MD5
DES & SHA1
DES

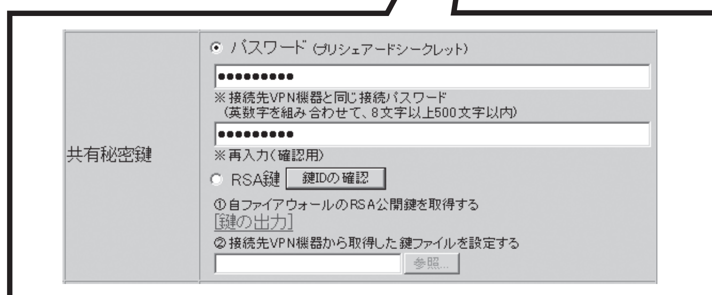
VPNパス(自動鍵交換:トンネルモード)画面

8. Phase1の「共有秘密鍵」を設定する。

IKEでの認証方法としてパスワードを利用するか、RSA鍵を利用するかを選択します。(VPNパスの概念図の⑤)



- パスワード(プリシェアードシークレット)
  事前に相手先と合意を取ったパスワード(プリシェアードシークレット)を用いて認証を行う場合は、「パスワード」を選択しテキストボックスにパスワードを入力します。
  パスワードは、接続先VPN機器と同じ接続パスワードとし、英数字を組み合わせて、8文字から500文字までで入力します。確認のため再入力してください。



VPNパス(自動鍵交換:トンネルモード)画面

- RSA鍵
  RSA鍵を利用する場合は、「RSA鍵」を選択しExpress5800/SG300が出力する鍵データと通信相手の機器が公開している鍵データの2つを設定します。

  ー 自ファイアウォールのRSA公開鍵を取得する
  「鍵の出力」をクリックしExpress5800/SG300のインストール時に作成した鍵をファイルに出力します。そのファイルを接続先VPN機器に渡して、RSA認証鍵として設定してください。

  ー 接続先VPN機器から取得した鍵を設定する
  接続先のVPN機器のRSA鍵を設定します。テキストボックスに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックしてファイルを選択してください。
  鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウで表示します。

✔ チェック

読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

ヒント

接続条件によっては、設定したアルゴリズムが使用されずIKEのネゴシエーションで自動選択されたアルゴリズムが使用されることがあります。

9. Phase2を設定する。

- 暗号化/認証
  AHを利用した認証を行う場合は、チェックボックスにチェックします。ハッシュアルゴリズムはMD5が適用されます。
  さらにESPで利用する暗号化アルゴリズムと認証アルゴリズム(ハッシュアルゴリズム)を設定します。

- 鍵の有効期間
  生成した鍵の有効期間(秒)を設定します。1200～86400秒まで設定することができます。

VPNパス(自動鍵交換：トンネルモード)画面

10. 必要なオプションのチェックボックスをチェックする。

- PFS(Perfect Forward Secrecy)の有効
  PFSを有効にします。PFSとは、万一、共有秘密鍵が解読された場合においても、VPN通信(IPSec)に利用する鍵(Phase2で生成)の解読ができないようにする方式です。

- IPSecで鍵更新を行う
  IPSecによるVPN通信で利用する鍵は、Phase2の項目で指定した有効期間を持ちます。「IPSecで鍵更新を行う」をチェックした場合、有効期間が切れた際に新たに鍵を生成して更新します。この機能により、鍵の有効期間を超えてVPN通信を継続することが可能になります。

- 適用時に有効化する
  「適用時に有効化する」をチェックした場合、設定の適用と同時にVPNの設定を行います。設定は行うもののVPN通信はまだ利用したくないというような場合は、「適用時に有効化する」をチェックせずに設定の適用を行ってください。

11. VPNパスに関する備考を入力する。

最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。

12. [適用]をクリックする。

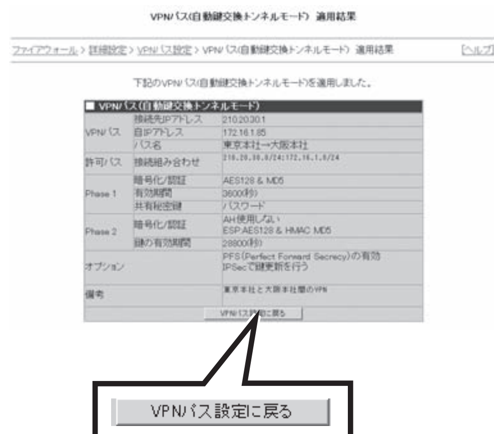
VPNパス(自動鍵交換：トンネルモード)適用結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

13. [VPNパス設定に戻る]をクリックする。

追加したVPNパスが反映されたVPNパス設定画面が表示されます。



VPNパス(自動鍵交換:トンネルモード)適用結果画面

ファイアウォール機能の設定方法

VPNパスの追加（自動鍵交換：トランスポートモード）

必要に応じてVPNパスを追加することができます。ここでは、トランスポートモードにおける自動鍵交換方式を利用したVPNパスの設定について説明します。VPN設定ウィザードでリモートアクセスVPNを設定した状態で新たなVPNパス（自動鍵交換：トランスポートモード）を追加するには、いったん設定済みのVPNパスを削除してから、以下の操作を行ってください。

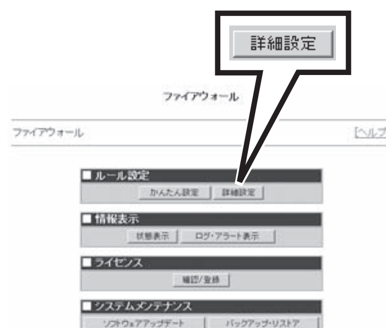
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

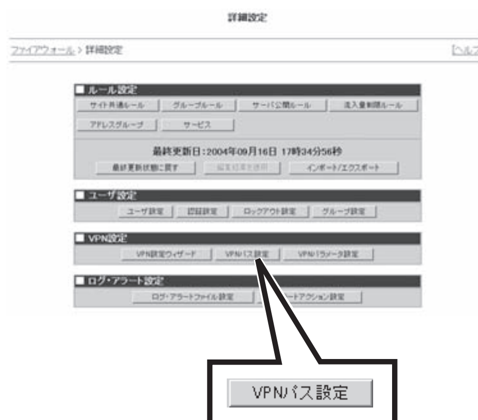
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

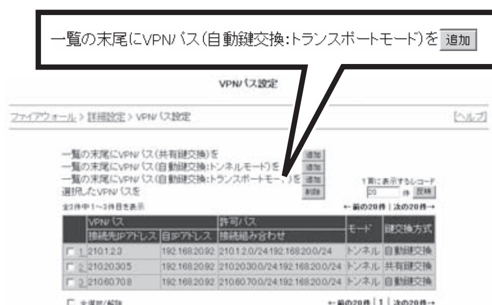
   VPNパス設定画面が表示されます。



詳細設定メニュー画面

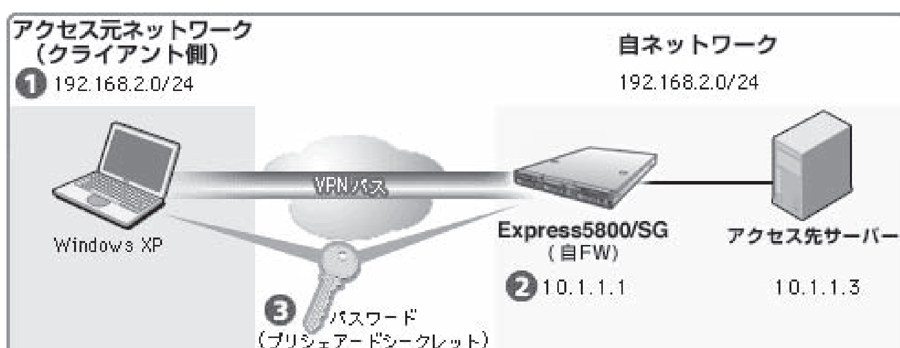
4. 「一覧の末尾にVPNパス(自動鍵交換:トランスポートモード)を『追加』」をクリックする。

VPNパス(自動鍵交換:トランスポートモード)画面が表示されます。



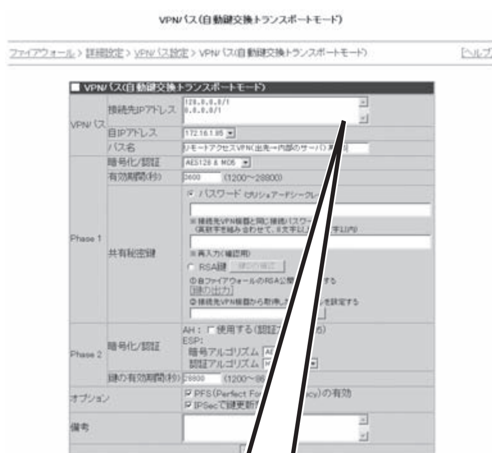
VPNパス設定画面

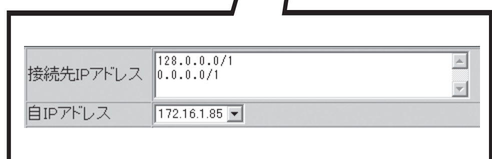
以降の各項目の設定手順では、VPN通信の概念を理解しやすくするために以下の図を用いて説明します。



5. VPNパスを設定する。

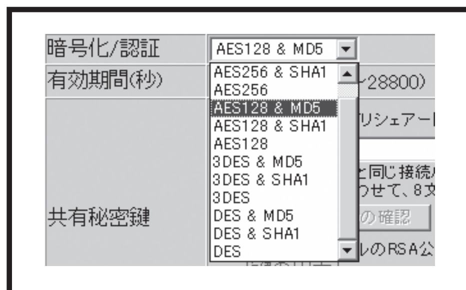
- 接続先アドレス
  VPNパスをはる接続先VPN機器が外部に公開しているIPアドレス、あるいはVPN機器が存在するネットワークアドレスを、一行に1つのアドレスの形式で入力します(VPNパスの概念図の①)。
- 自IPアドレス
  VPNパスをはる接続先から参照することができる、Express5800/SG300の外部ネットワークにつなげたインタフェースのIPアドレスをプルダウンメニューから選択します(VPNパスの概念図の②)。
- パス名
  VPNパスを識別する任意の文字列を指定します。VPNパス名は自由に設定することができます。最大で256バイトまでの文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。





VPNパス(自動鍵交換:トランスポートモード)画面

6. Phase1の「暗号化/認証」と「有効期間」を設定する。

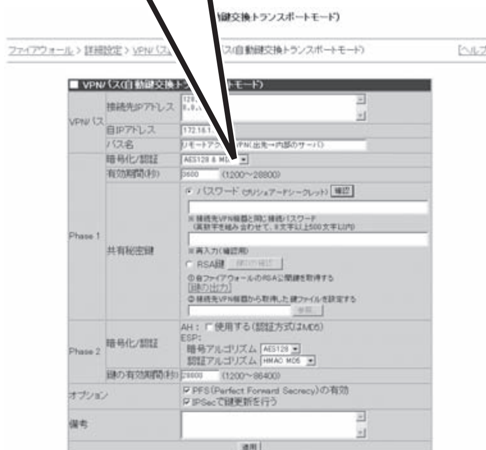




自動鍵交換方式では、最初にIKEを使って通信相手を認証し、暗号化アルゴリズムと暗号鍵を決定します。事前にパスワードまたはRSA鍵を共有していることが条件になります。

IKEでは、まずハッシュアルゴリズムとパスワード(またはRSA鍵)を使って通信相手双方の認証を行います。認証完了後、暗号通信を利用して鍵の元となる乱数データと暗号化アルゴリズムを通知しあい、実際の通信で使用する共通鍵(秘密鍵)を生成します。

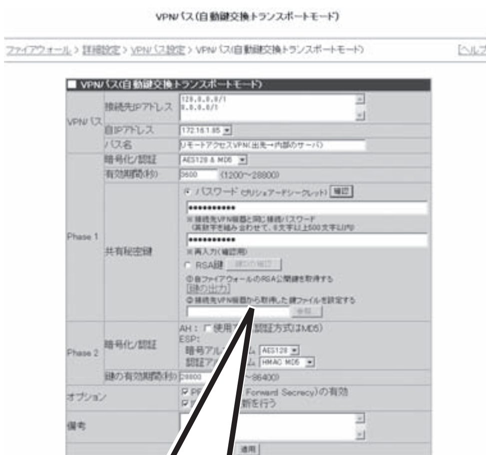
- 暗号化/認証
  IKEの暗号化に利用する暗号化アルゴリズムと認証に利用するハッシュアルゴリズムを設定します。
- 有効期間
  認証完了後の有効期間(秒)を設定します。1200～28800秒まで設定することができます。

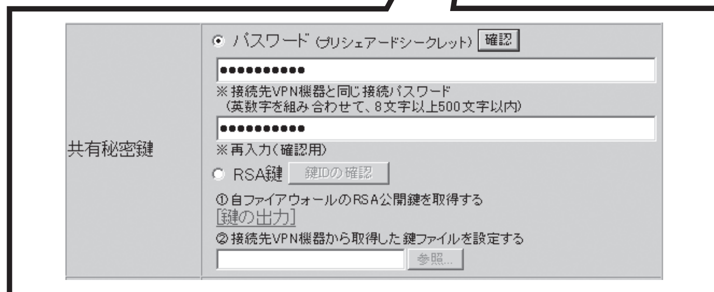


VPNパス(自動鍵交換：トランスポートモード)画面

7. Phase1の「共有秘密鍵」を設定する。

IKEでの認証方法としてパスワードを利用するかRSA鍵を利用するかを選択します。(VPNパスの概念図の③)





VPNパス(自動鍵交換：トランスポートモード)画面

- パスワード(プリシェアードシークレット)
  事前に相手先と合意を取ったパスワード(プリシェアードシークレット)を用いて認証を行う場合は、「パスワード」を選択しテキストボックスにパスワードを入力します。
  パスワードには必ずアルファベットと数字の両方が含まれている必要があります。どちらか一方のみで構成されるパスワードは入力できません。確認のため再入力してください。

- RSA鍵
  RSA鍵を利用する場合は、「RSA鍵」を選択しExpress5800/SG300が出力する鍵データと通信相手の機器が公開している鍵データの2つを設定します。

  ー 自ファイアウォールのRSA公開鍵を取得する
  「鍵の出力」をクリックしExpress5800/SG300のインストール時に作成した鍵をファイルに出力します。そのファイルを接続先VPN機器に渡して、RSA認証鍵として設定してください。

  ー 接続先VPN機器から取得した鍵を設定する
  接続先のVPN機器のRSA鍵を設定します。テキストボックスに、接続先VPN機器から出力した鍵ファイル名を指定します。ファイル名を直接入力するか、[参照]をクリックして、ファイルを選択してください。
  鍵ファイル名を指定した後、[鍵IDの確認]をクリックすると、鍵IDの確認画面を別ウィンドウで表示します。

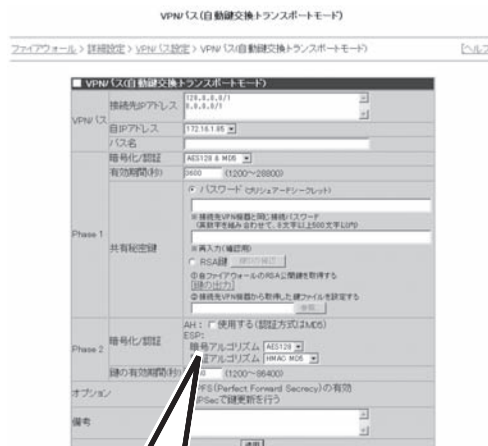
> **チェック**
>
> 読み込む鍵ファイルは、ファイアウォールが動作している端末ではなく、Management Consoleを表示している管理クライアント上に保存してください。

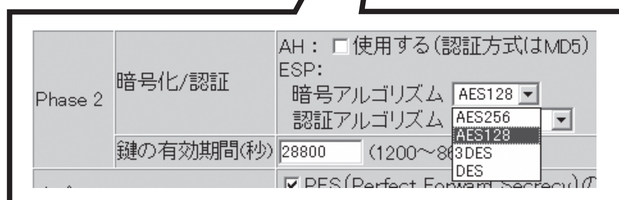
> **ヒント**
>
> 接続条件によっては、設定したアルゴリズムが使用されずIKEのネゴシエーションで自動選択されたアルゴリズムが使用されることがあります。

8. Phase2を設定する。

- 暗号化/認証
  AHを利用した認証を行う場合は、チェックボックスにチェックします。ハッシュアルゴリズムはMD5が適用されます。
  さらにESPで利用する暗号化アルゴリズムと認証アルゴリズム(ハッシュアルゴリズム)を設定します。

- 鍵の有効期間
  生成した鍵の有効期間(秒)を設定します。1200～86400秒まで設定することができます。





VPNパス(自動鍵交換：トランスポートモード)画面

9. 必要なオプションのチェックボックスをチェックする。

- PFS(Perfect Forward Secrecy)
  PFSを有効にします。PFSとは、万一、共有秘密鍵が解読された場合においても、VPN通信(IPSec)に利用する鍵(Phase2で生成)の解読ができないようにする方式です。
- IPSecで鍵更新を行う
  IPSecによるVPN通信で利用する鍵は、Phase2の項目で指定した有効期間を持ちます。「IPSecで鍵更新を行う」をチェックした場合、有効期間が切れた際に新たに鍵を生成して更新します。この機能により、鍵の有効期間を超えてVPN通信を継続することが可能になります。

10. VPNパスに関する備考を入力する。

最大で2048バイトまでの任意の文字列を受け付けますが、二重引用符(")およびカンマ(,)を含めることはできません。入力は任意です。

11. [適用]をクリックする。

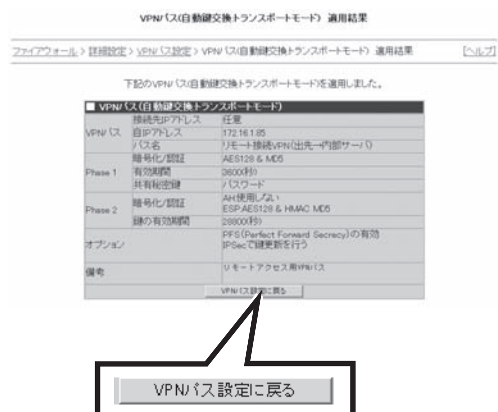
VPNパス(自動鍵交換：トランスポートモード)適用結果画面が表示されます。



登録に失敗した場合には、エラー内容を示す画面を表示します。

12. [VPNパス設定に戻る]をクリックする。

追加したVPNパスが反映されたVPNパス設定画面が表示されます。



VPNパス(自動鍵交換：トランスポートモード)適用結果画面

VPNパスの削除

不要になったVPNパスを削除することができます。

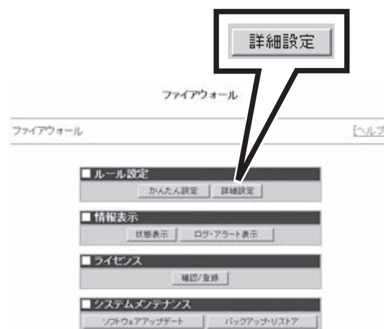
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

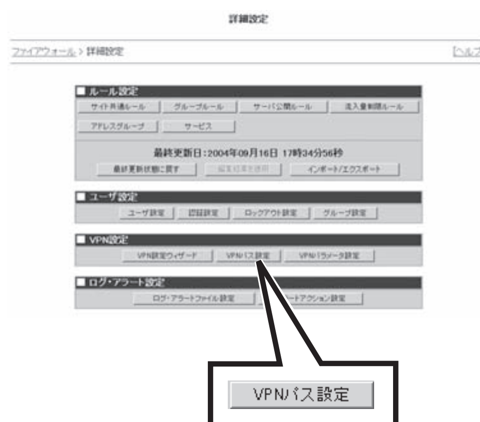
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

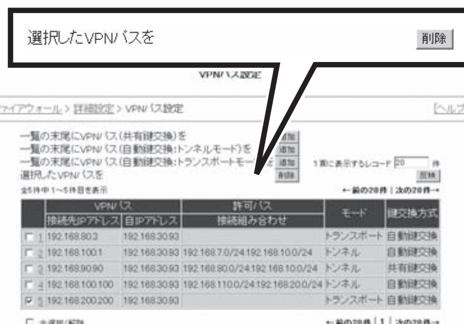
   VPNパス設定画面が表示されます。



詳細設定メニュー画面

4. 削除したいVPNパス番号の横に表示されるチェックボックスをチェックし、「選択したVPNパスを『削除』」をクリックする。

VPNパス削除確認画面が表示されます。

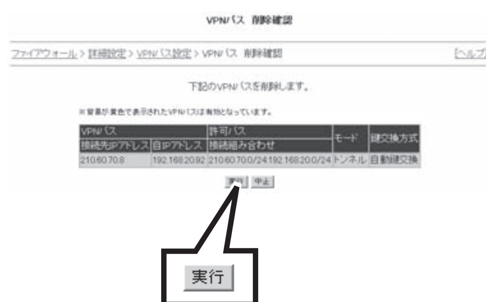


VPNパス設定画面



「全選択/解除」のチェックボックスをチェックすると、削除可能なVPNパスのすべてを一度に選択できます。逆に、「全選択/解除」のチェックボックスのチェックを外すと、いったんチェックボックスにチェックをつけたすべてのVPNパスを削除対象から外すこともできます。

5. ［実行］をクリックする。



VPNパス削除確認画面



- 背景が黄色で表示されたVPNパスは有効となっているVPNパスです。
- 背景が赤色で表示されたVPNパスはグループルールで使用中です。まずグループルールの方からVPNパスを解除し、グループルールを適用してから、再度VPNパス削除を行う必要があります。
- [中止]をクリックすると、削除されずにVPN情報一覧画面に戻ります。

VPNパス削除結果画面が表示されます。

6. ［VPNパス設定に戻る］をクリックする。



VPNパス削除結果画面



背景が黄色で表示されたVPNパスは削除に失敗したVPNパスです。

VPNパスが削除され、削除が反映したVPNパス設定画面が表示されます。



現在有効なVPNパスを削除すると、そのVPNパスを使用して行っている通信も切断されます。

VPNパスの更新

一度設定したVPNパスの設定内容を変更することができます。

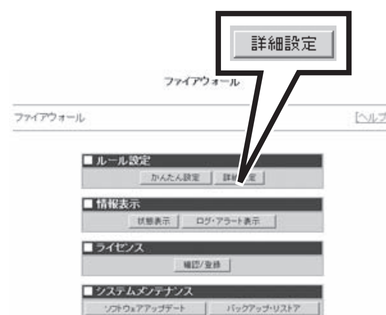
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

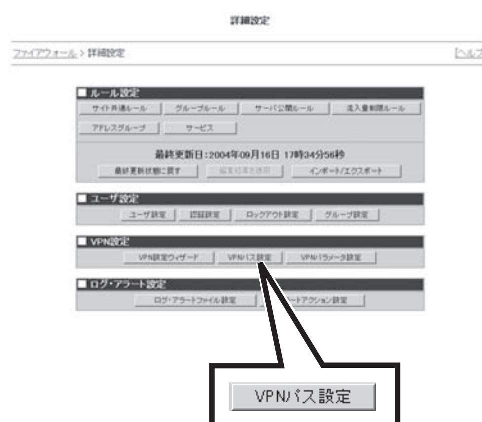
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「VPN設定」から[VPNパス設定]をクリックする。

   VPNパス設定画面が表示されます。



詳細設定メニュー画面

4. 変更したいVPNパスの番号をクリックする。

   変更したいVPNパスのモード、鍵交換方式にしたがったVPNパス更新画面が表示されます。





VPNパス設定画面

5. 表示される各項目を設定する。

   それぞれの設定内容は追加設定と同様です。

6. ［適用］をクリックする。

   VPNパス適用結果画面が表示されます。

> チェック
>
> 登録に失敗した場合には、エラー内容を示す画面を表示します。

VPNパス更新画面

7. ［VPNパス設定に戻る］をクリックする。

   変更したVPNパスが反映されたVPNパス設定画面が表示されます。

> 重要
>
> **現在有効なVPNパスを更新すると、そのVPNパスを使用して行っている通信も切断されることがあります。**

VPNパス適用結果画面

VPNパラメータの設定

Express5800/SG300で同時に利用できるVPNトンネル数、トランスポート数を設定することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

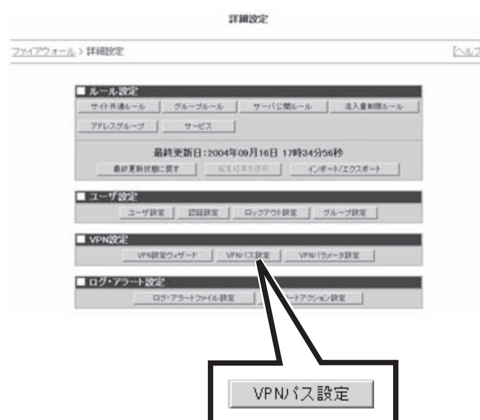
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

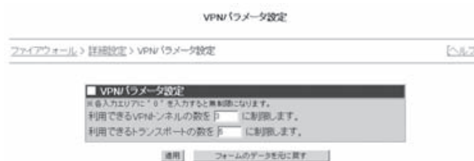
3. 詳細設定メニューの「VPN設定」から[VPNパラメータ設定]をクリックする。

   VPNパラメータ設定画面が表示されます。



詳細設定メニュー画面

4. 利用できるVPNトンネルの数、トランスポートの数をそれぞれテキストボックスに入力する。



VPNパラメータ設定画面



- **値は0～65535まで設定することができます。0を設定すると無制限になります。**
- **ユーザログインにより有効となったトランスポートモードのセッションは、セッションの有効期間終了後、鍵の有効期間が切れるまでが、トランスポート数の計算対象となります。**

5. [適用]をクリックする。



[フォームのデータを元に戻す]をクリックすると、前回設定した値に戻ります。

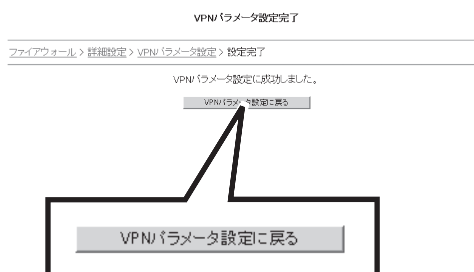
VPNパラメータ設定完了画面が表示されます。



[適用]をクリックするとVPNの接続が一時切断されます。

6. [VPNパラメータ設定に戻る]をクリックする。

VPNパラメータ設定画面が表示されます。



VPNパラメータ設定完了画面

ログ・アラート設定

Express5800/SG300が出力するログファイル、アラートファイルに関連する各種パラメータを設定することができます。
ログ・アラート設定では以下の項目を設定することができます。

ログ・アラートファイル設定 .... Express5800/SG300が出力するログファイル、アラートファイルのパラメータを設定します。

ログ・アラートファイルダウンロード/アップロード .... ログ・アラートファイルを管理クライアントにダウンロードしたり、ダウンロードしたファイルをExpress5800/SG300にアップロードします。

アラートアクション設定 .... アラート発生時のアクションを設定します。

ログ・アラートファイル設定

Express5800/SG300が出力するログファイル、アラートファイルの収集時間や出力内容などの各種パラメータを設定することができます。

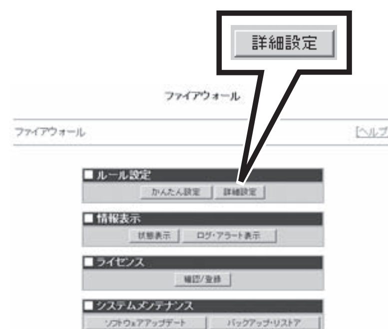
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

ファイアウォール機能の設定方法

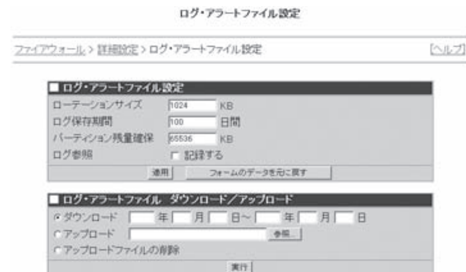
3. 詳細設定メニューの「ログ・アラート設定」から[ログ・アラートファイル設定]をクリックする。

   ログ・アラートファイル設定画面が表示されます。



詳細設定メニュー画面

4. ログ・アラートファイル設定画面に表示される各項目を設定する。



ログ・アラートファイル設定画面

設定	ローテーションサイズ	1つのファイルの最大サイズを4096KB(4MB)から65536KB(64MB)の範囲で指定します。 通常ログファイルは1日単位でローテーションを行いますが、ログファイルサイズが指定サイズを超えた場合には、1日単位のローテーションとは別にローテーションを行います。
	ログ保存期間	ファイルを残す日数を指定します。1日から2000日までの範囲で指定します。 なお、ログを保存しているパーティションの残量が少なくなった場合には、下記の残量確保の設定により、古いログファイルから削除されます。 この場合、指定した保存期間に達する前に削除されます。
	パーティション残量確保	ログを出力するシステムのパーティションに確保する空き容量を指定します。パーティション容量が指定値以下になると、古いログから順に指定残量が確保できるまで削除します。 32768KB(32MB)から1048576KB(1GB)までの範囲で指定します。
	ログ参照	チェックすると、ログを参照したときに参照情報をログとして記録します。

5. [適用]をクリックする。



[フォームのデータを元に戻す]をクリックすると、適用前の設定値に戻ります。

6. 別ウィンドウで更新確認ダイアログメッセージが表示されるので、[OK]をクリックする。

ログ・アラートファイルダウンロード／アップロード

ログ・アラートファイルを管理クライアントにダウンロードしたり、ダウンロードしたファイルをExpress5800/SG300にアップロードすることができます。

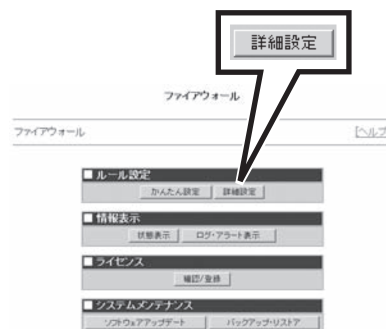
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

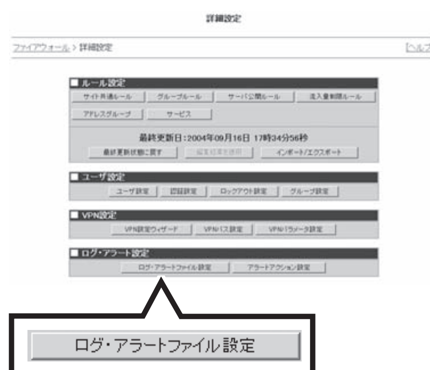
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

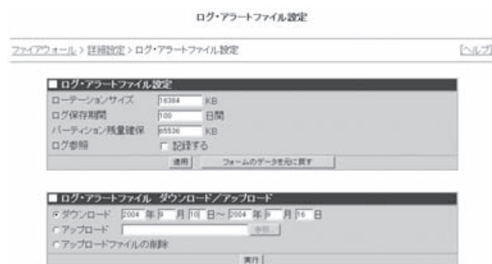
3. 詳細設定メニューの「ログ・アラート設定」から[ログ・アラートファイル設定]をクリックする。

   ログ・アラートファイル設定画面が表示されます。



詳細設定メニュー画面

4. ログ・アラートファイルダウンロード／アップロードメニューから実行する操作を選択する。



ログ・アラートファイル設定画面

ダウンロード/ アップロード	ダウンロード	日付指定でログ・アラートファイルをコンソール端末上にダウンロードします。
	アップロード	ログファイルを指定してExpress5800/SG300にアップロードします。アップロードされたファイルはログ保存期間を過ぎても残されます。またパーティション残量確保時でも削除対象となりません。なお、アップロードにより保存されるファイルは1ファイルのみです。新しいファイルをアップロードすると保存されているファイルは削除されます。アップロードしたファイルは「ログ・アラート表示」から確認できます。「ログ・アラート表示」については、285ページを参照してください。
	アップロード ファイルの削除	アップロードされているファイルを削除します。

5. ［実行］をクリックする。

指定した操作が実行されます。

●ダウンロード

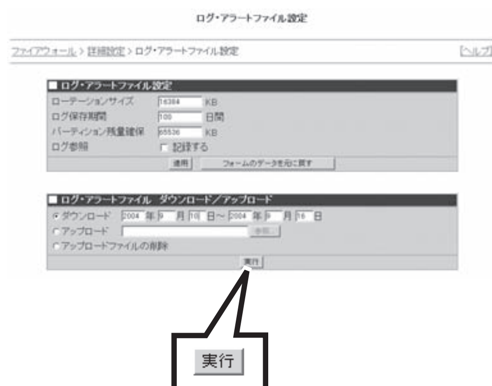
ファイルのダウンロード画面が表示されるので[保存]をクリックして、保存場所を指定します。

●アップロード

［参照］をクリックしてファイルを指定してから[実行]をクリックします。確認画面が表示されるので[OK]をクリックします。

●アップロードファイルの削除

別ウィンドウで削除確認のダイアログメッセージが表示されるので[OK]をクリックします。別ウィンドウで完了確認のダイアログメッセージが表示されるので[OK]をクリックします。



ログ・アラートファイル設定画面

アラートアクション設定

アラート出力時に行うアクションの設定を行います。

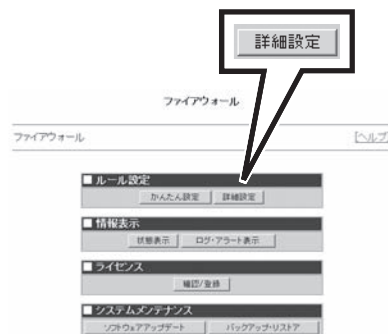
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「ルール設定」から[詳細設定]をクリックする。

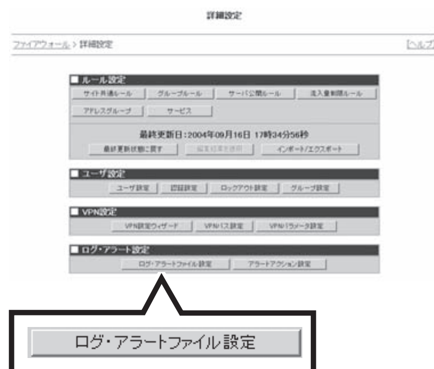
   詳細設定メニュー画面が表示されます。



ファイアウォールメニュー画面

3. 詳細設定メニューの「ログ・アラート設定」から[アラートアクション設定]をクリックする。

   アラートアクション設定画面が表示されます。



詳細設定メニュー画面

4. アラートアクション設定画面に表示される各項目を設定する。

項　目		説　明
通知方法	メール送付	アラート発生をメールにて通知します。通知するメールアドレスを3つまで登録できます。「送信元アドレス」には、メールの送信元を指定できます。
	SYSLOG出力	アラート発生をSYSLOGで出力します。出力するファシリティとレベルを設定します。
	コマンド実行	アラート発生時にコマンドを実行します。実行するコマンドを登録します。
通知間隔		通知間隔を60秒から86400秒までの範囲で指定します。
メッセージ	同一出力の抑制	チェックすると、同様のアラートが「通知間隔」で指定した間に発生した時に、アクションの実行を抑制するとともに、メール通知、もしくはsyslogの出力で同様のアラートが連続した回数のみ出力されても、最初のアラートを一度だけ出力するようになります。
	アドバイザリの出力（メールのみ）	チェックすると、アラートについての対処方法を含んだメッセージを送ります。ただし、この機能は、「メール送付」による通知でのみ有効です。
通知イベント		イベントごとに行うアクションのチェックボックスをチェックすることで設定します。メール1はメール送付の「アドレス1」、メール2は「アドレス2」にメールを送信することを意味しています。

アラートアクション設定画面

ヒント

[通知イベント]にある[自動防御]は、[SYN-SCAN検出]と[PING-SWEEP検出]イベントについて選択できるオプションです。このオプションを有効にすると、[SYN-SCAN検出]、または[PING-SWEEP検出]イベントを検出した際、Express5800/SG300は自動的に送信元との通信を一時的に遮断します。

5. [更新]をクリックする。



- [フォームのデータを元に戻す]をクリックすると、適用前の設定値に戻ります。
- メールアドレス部分には、必ず有効なメールアドレスを指定してください。
  メールの送信時にはアドレスのチェックは行わないため、不正なアドレスが指定された場合、メールはそのまま送信され、エラーになる場合があります。

6. 更新結果ダイアログメッセージが表示されるので[OK]をクリックする。

   アラートアクションが設定されます。

情報表示

Express5800/SG300の情報を表示することができます。
情報表示では以下の項目を表示することができます。

状態表示 .... Express5800/SG300の状態を表示することができます。

ログ・アラートの表示 .... Express5800/SG300の出力するログおよびアラート情報を表示することができます。

状態表示

Express5800/SG300が正常に起動中であるか、あるいは異常状態であるかを表示することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

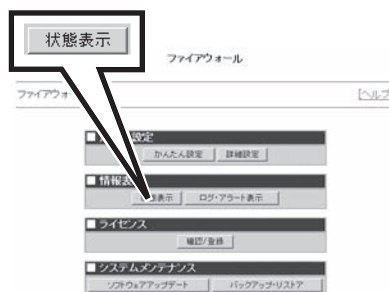
   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「情報表示」から[状態表示]をクリックする。

   状態表示画面が表示されます。以下のような状態が表示されます。

   - 現在、正常動作中
     Experess5800/SG300はファイアウォール装置として正常に稼動中です。
   - 現在、停止中
     ファイアウォールは停止しています。
   - 現在、障害発生中
     何らかの原因によりファイアウォールに障害が発生しており、一部機能が停止しています。
     次ページの「ログ・アラート表示」を参照してエラーが出ていないか確認してください。
     なお、状態の右側に表示される以下のボタンをクリックすることで、Experess5800/SG300を起動、再起動、停止することができます。
   - 現在、現用中
     二重化構成時、運用系の機器として正常に稼働中です。
   - 現在、待機中
     二重化構成時、待機系の機器としてホットスタンバイしています。



ファイアウォールメニュー画面



状態表示画面

- 停止する
  Experess5800/SG300が停止中以外の場合にクリックすると停止します。
- 再起動する
  クリックするとExperess5800/SG300を再起動します。
- 起動する
  Experess5800/SG300の停止時にクリックすると起動します。

ログ・アラート表示

Express5800/SG300が出力するログ情報およびアラート情報を表示/出力することができます。以下のような表示/出力をすることができます。

- ログ表示
- CSV出力
- 簡易集計表示
- 外部統計用CSV出力

ログ表示

Express5800/SG300が出力するログ情報およびアラート情報を表示することができます。

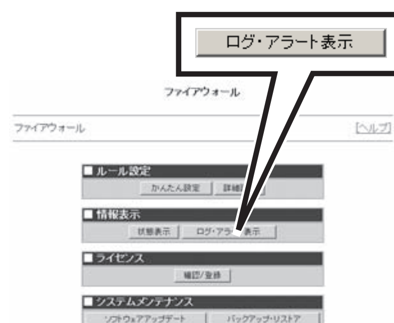
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



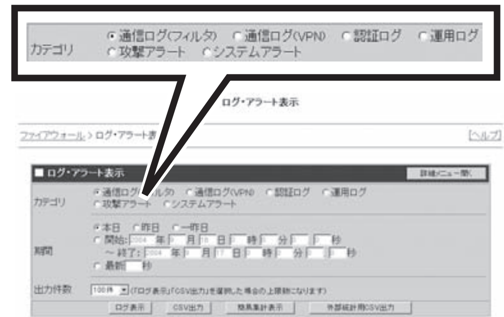
2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。

   ログ・アラート表示画面が表示されます。



ファイアウォールメニュー画面

3. 表示するログのカテゴリを選択する。



ログ・アラート表示画面

- 通信ログ(フィルタ)
  フィルタリング機能によるパケットの通過、拒否、破棄のログを表示します。表示される通信は、サイト共通ルール、グループルールで、ログを記録すると設定したもののみです。
- 通信ログ(VPN)
  VPNパスを利用した通信のログを表示します。
- 認証ログ
  ユーザ認証のログを表示します。
- 運用ログ
  Express5800/SG300の起動や停止など運用情報のログを表示します。
- 攻撃アラート
  Express5800/SG300が攻撃を検出したときに出力するアラート情報です。
- システムアラート
  Express5800/SG300の運用上のアラート情報です。

4. 期間を選択する。

「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログを表示します。
それ以外の日や数日に渡ってログを取得する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを表示します。

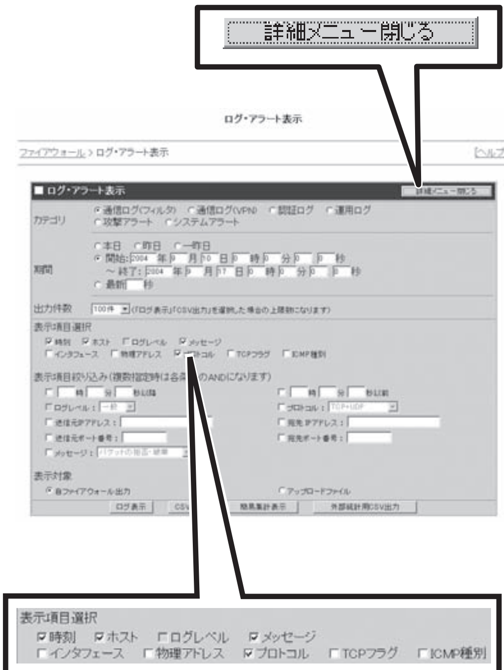
5. 表示するログの上限となる「出力件数」をプルダウンメニューから選択する。

6. さらに詳しく条件を設定する場合はタイトルバーの右側にある[詳細メニュー開く]をクリックする。

詳細メニューが表示されます。



- 特に詳細条件を指定しない場合は手順8に進みます。
- [詳細メニュー閉じる]をクリックすると詳細メニューが閉じます。



ログ・アラート表示(詳細メニュー)画面

7. ログの表示条件の詳細な設定を行う。

カテゴリ	項　目		説　明
通信ログ（フィルタ）	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
		インタフェース	チェックすると通信のインタフェースが表示されます。
		物理アドレス	チェックするとインタフェースの物理アドレスが表示されます。
		プロトコル	チェックすると通信種別が表示されます。
		TCPフラグ	TCP通信の場合、チェックするとフラグの状態が表示されます。
		ICMP種別	ICMP通信の場合、チェックすると通信種別が表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		プロトコル	表示するプロトコルをプルダウンメニューから選択します。
		送信元IPアドレス	表示する送信元IPアドレスを指定します。
		送信元ポート番号	表示する送信元ポート番号をプルダウンメニューから選択します。
		宛先IPアドレス	表示する宛先IPアドレスを指定します。
		宛先ポート番号	表示する宛先ポート番号を指定します。
		メッセージ	チェックしてメッセージの種類を選択します。
通信ログ（VPN通信）運用ログ認証ログ	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		ログレベル	チェックするとログレベルが表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		ログレベル	表示するログレベルをプルダウンメニューから指定します。
攻撃アラート	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
システムアラート	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
すべて	表示対象	自ファイアウォール出力	自ファイアウォール（Express5800/SG300）が出力したファイルを表示します。
		アップロードファイル	Express5800/SG300にアップロードしたファイルを表示します。

8. ［ログ表示］をクリックする。

指定した条件のログ情報が別ウィンドウで表示されます。



- 「キーワードサーチ」のテキストボックスにキーワードを入力し[検索]をクリックすると、検索した条件のログのみを表示します。検索した条件に当てはまらないログは一覧に表示されません。また、2つ以上の条件検索はすることができません。
- 表中のヘッダ（背景緑色の部分）をクリックすると、その列でソートすることができます。
- キーワードサーチやソートの対象となるのは、そのとき画面に表示されているもののみです。

期間の指定で「最新」を選択した場合は、オートリフレッシュ機能が利用できます。「オートリフレッシュ」のチェックボックスにチェックすると、5秒ごとに自動的にログを再取得し、表示を更新します。ただし、この場合は、キーワードサーチとソートを行うことはできません。

9. ［このウィンドウを閉じる］をクリックする。

ログ情報表示画面が閉じます。



ログ情報表示画面

CSV出力

Express5800/SG300が出力するログ情報をCSVファイルに出力することができます。

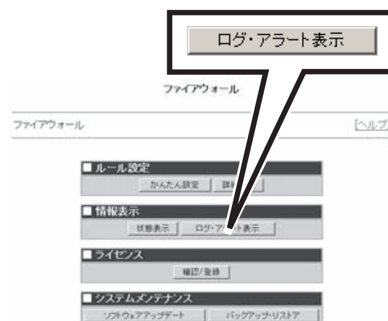
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。

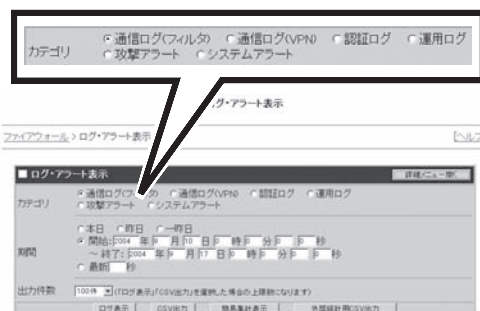
   ログ・アラート表示画面が表示されます。



ファイアウォールメニュー画面

3. CSVファイルに出力するログのカテゴリを選択する。

   - 通信ログ(フィルタ)
     フィルタリング機能によるパケットの通過、拒否、破棄のログをCSVファイルに出力します。CSVファイルに出力される通信は、サイト共通ルール、グループルールで、ログを記録すると設定したもののみです。
   - 通信ログ(VPN)
     VPNパスを利用した通信のログをCSVファイルに出力します。
   - 認証ログ
     ユーザ認証のログをCSVファイルに出力します。
   - 運用ログ
     Experess5800/SG300の起動や停止など運用情報のログをCSVファイルに出力します。
   - 攻撃アラート
     Express5800/SG300が攻撃を検出したときに出力するアラート情報です。
   - システムアラート
     Express5800/SG300の運用上のアラート情報です。



ログ・アラート表示画面

4. 期間を選択する。

   「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログをCSVファイルに出力します。
   それ以外の日や数日に渡ってログを出力する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
   「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを出力します。

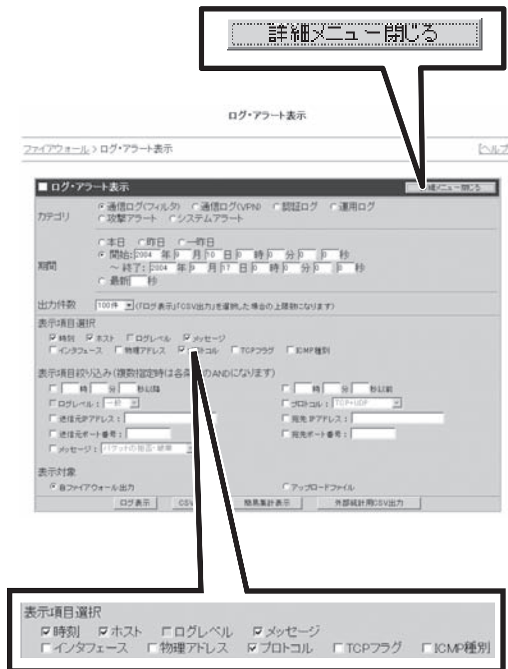
5. 出力するログの上限となる「出力件数」をプルダウンメニューから選択する。

6. さらに詳しく条件を設定する場合はタイトルバーの右側にある[詳細メニュー開く]をクリックする。

   詳細メニューが表示されます。

 ヒント

- 特に詳細条件を指定しない場合は手順8に進みます。
- [詳細メニュー閉じる]をクリックすると詳細メニューが閉じます。



ログ・アラート表示(詳細メニュー)画面

7. ログの出力条件の詳細な設定を行う。

カテゴリ	項　目		説　明
通信ログ（フィルタ）	表示項目選択	時刻	チェックすると時刻が出力されます。
		ホスト	チェックするとホスト名が出力されます。
		メッセージ	チェックするとメッセージが出力されます。
		インタフェース	チェックすると通信のインタフェースが出力されます。
		物理アドレス	チェックするとインタフェースの物理アドレスが出力されます。
		プロトコル	チェックすると通信種別が出力されます。
		TCPフラグ	TCP通信の場合、チェックするとフラグの状態が出力されます。
		ICMP種別	ICMP通信の場合、チェックすると通信種別が出力されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		プロトコル	表示するプロトコルをプルダウンメニューから選択します。
		送信元IPアドレス	表示する送信元IPアドレスを指定します。
		送信元ポート番号	表示する送信元ポート番号を指定します。
		宛先IPアドレス	宛先IPアドレスを指定します。
		宛先ポート番号	宛先ポート番号を指定します。
		メッセージ	チェックしてメッセージの種類を選択します。
運用ログ 認証ログ 通信ログ（VPN通信）	表示項目選択	時刻	チェックすると時刻が出力されます。
		ホスト	チェックするとホスト名が出力されます。
		ログレベル	チェックするとログレベルが出力されます。
		メッセージ	チェックするとメッセージが出力されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
		ログレベル	表示するログレベルをプルダウンメニューから指定します。
攻撃アラート	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
システムアラート	表示項目選択	時刻	チェックすると時刻が表示されます。
		ホスト	チェックするとホスト名が表示されます。
		メッセージ	チェックするとメッセージが表示されます。
	表示項目絞り込み	時刻	表示する時刻を「以降」「以前」で指定します。
すべて	表示対象	自ファイアウォール出力	自ファイアウォール(Express5800/SG300)が出力したファイルをCSV出力します。
		アップロードファイル	Express5800/SG300にアップロードしたファイルをCSV出力します。

8. [CSV出力]をクリックする。

CSVファイルの保存画面が表示されるので保存先を決定します。

簡易集計表示

Express5800/SG300が保存している通信ログ情報を簡易集計し、グラフィカルに表示することができます。

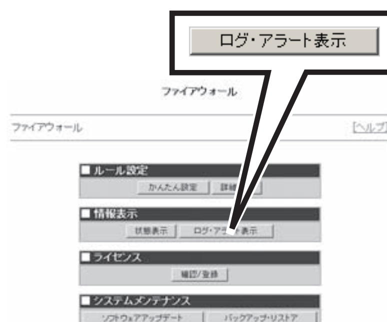
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。

   ログ・アラート表示画面が表示されます。



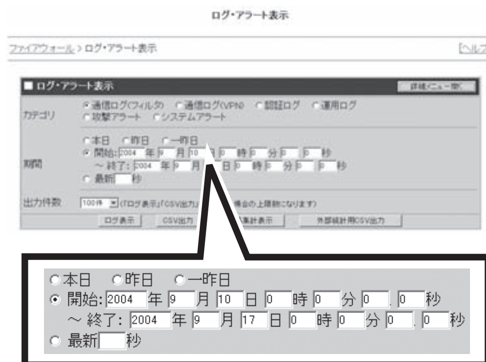
ファイアウォールメニュー画面

3. 期間を選択する。

   「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログを表示します。
   それ以外の日や数日に渡ってログを取得する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
   「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを表示します。



簡易集計表示では、「期間」以外の項目は指定できません。



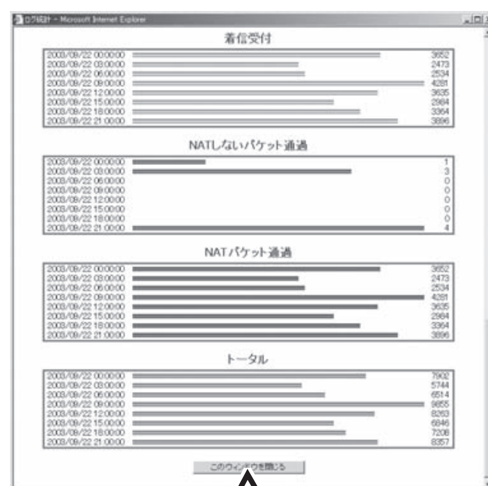
ログ・アラート表示画面

4. [簡易集計表示]をクリックする。

   指定した日付のログ情報の簡易集計が別ウィンドウで表示されます。

5. ［このウィンドウを閉じる］をクリックする。

簡易集計表示画面が閉じます。



簡易集計表示画面

ファイアウォール機能の設定方法

外部統計用CSV出力

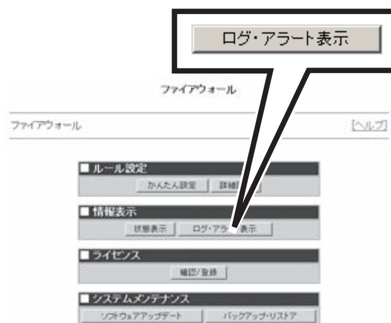
外部集計ツールで利用するCSVファイルを出力することができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。

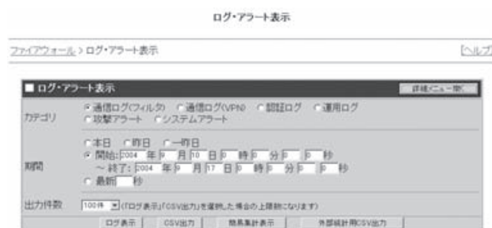
2. ファイアウォールメニューの「情報表示」から[ログ・アラート表示]をクリックする。

   ファイアウォールメニュー画面

   ログ・アラート表示画面が表示されます。

3. 期間を選択する。

   ログ・アラート表示画面

   「本日」、「昨日」、「一昨日」をクリックするとそれぞれ指定した一日分のログをCSVファイルに出力します。
   それ以外の日や数日に渡ってログを出力する場合は、「開始」のラジオボタンを選択し、開始から終了までの年月日時分秒を指定します。
   「最新」をクリックしてテキストボックスに秒を設定すると、指定した直近の秒までのログを出力します。

   外部統計用CSV出力では、「期間」以外の項目は指定できません。

4. [外部統計用CSV出力]をクリックする。

   CSVファイルの保存画面が表示されるので保存先を決定します。

ライセンスの確認と登録

Express5800/SG300を利用するには、ライセンスキーの登録を行う必要があります。またサポートキーを登録すると、ソフトウェアおよびOSのサポートサービスを受けることができます。ライセンスキー、サポートキーの取得については、1章の「ライセンスキー」および「ソフトウェアサポートサービス」を参照してください。

ライセンスキー／サポートキーの登録

Express5800/SG300では、ファイアウォールとして動作させるために必要なライセンスキーと、サポートサービスを受けるために必要なサポートキーの2種類のキーによりライセンスを管理しています。
Express5800/SG300を利用するには、はじめにライセンスの登録を行う必要があります。

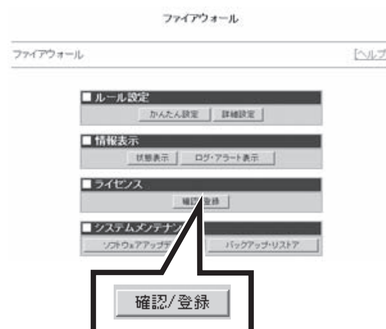
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. 「ファイアウォール」メニューの「ライセンス」から[確認/登録]をクリックする。

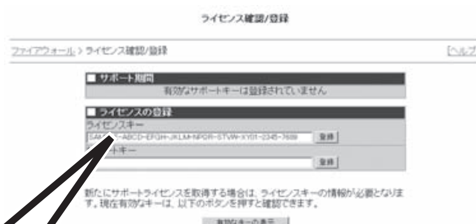
   ライセンスの確認と登録画面が表示されます。

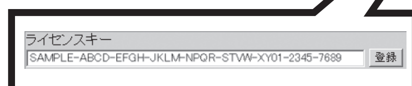


ファイアウォールメニュー画面

3. 「ライセンスキー」のテキストボックスに購入先より通知されたライセンスキーを入力し、[登録]をクリックする。

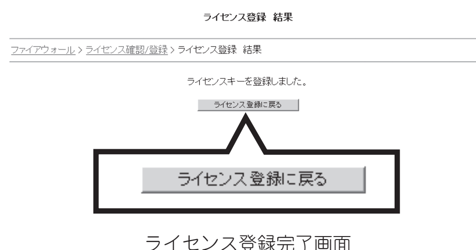
   ライセンスの登録完了画面が表示されます。





ライセンス確認/登録画面

4. ［ライセンス登録に戻る］をクリックする。



ライセンス登録完了画面

5. ソフトウェアサポートサービスを購入している場合は、「サポートキー」のテキストボックスに購入先より通知されたサポートキーを入力し、［登録］をクリックする。

   ライセンスの登録完了画面が表示されます。

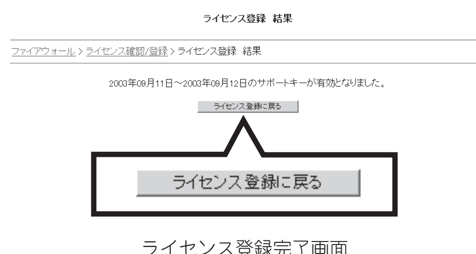
サポートキー
SAMPLE-ABCD-EFGH-JKLM-NPQR-STVW-XY01-2345-7689 登録

ライセンス確認/登録画面

6. ライセンスの有効期限を確認し［ライセンス確認/登録に戻る］をクリックする。

重要

サポートキーはライセンスキーを登録していないと登録できません。



ライセンス登録完了画面

ライセンス設定の確認

登録したライセンスキー/サポートキーを確認することができます。

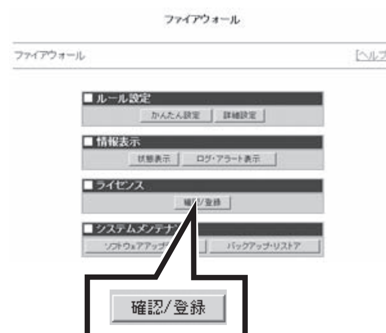
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   「ファイアウォール」メニュー画面が表示されます。



2. 「ファイアウォール」メニューでライセンスの[確認/登録]をクリックする。

   ライセンスの確認と登録画面が表示されます。



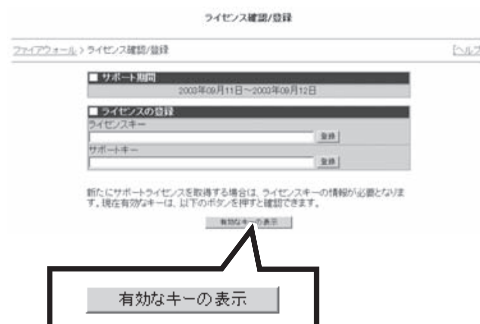
ファイアウォールメニュー画面

3. [有効なキーの表示]をクリックする。

   ライセンスの確認画面が表示され、有効なライセンスキー、およびサポートキーが確認できます。



登録済みのライセンスキーであっても有効期限切れや無効のキーは表示されません。



ライセンス確認/登録画面



有効なライセンス表示画面

システムメンテナンス

管理者は、Express5800/SG300のソフトウェアのアップデートや、設定したルール、グループ情報などのデータのバックアップ／リストアをすることができます。

ソフトウェアアップデート

ソフトウェアサポートサービスを購入している場合は、インターネットを利用してソフトウェアおよびOSを利用可能な最新状態へアップデートすることができます。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「システムメンテナンス」から[ソフトウェアアップデート]をクリックする。

   サポートサービスユーザ認証画面が表示されます。



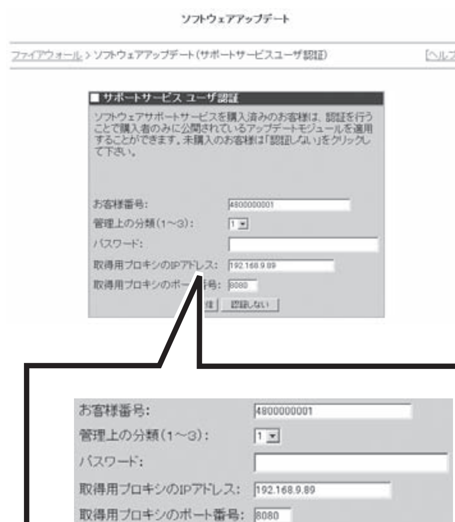
ファイアウォールメニュー画面

3. 画面に従い以下の項目を入力する。

   - お客様番号
   - 管理上の分類
   - パスワード



お客様番号、管理上の分類番号、パスワードは製品購入時に通知されたものを入力します。お客様番号はライセンス登録を行っていれば自動的に表示されます。



サポートサービスユーザ認証画面

4. 外部ネットワークへ通信するためにプロキシを利用している場合は、以下の項目についても入力する。

- 取得用プロキシのIPアドレス
- 取得用プロキシのポート番号



プロキシを利用していない場合は空欄のままにしておきます。

重要

サポートサービスユーザ認証画面を表示しているブラウザも、アップデートパッケージの情報を取得するためにサポートサービスサイトに直接アクセスを行います。そのため、事前に管理クライアントからの外部ネットワークへのHTTP通信を許可しておく必要があります。フィルタリングの設定については121ページの「サイト共通ルール」を参照してください。

また、インターネットへ通信するためにHTTPプロキシの設定が必要な場合は、ブラウザ自身にプロキシの設定を行ってください。

5. ［送信］をクリックする。

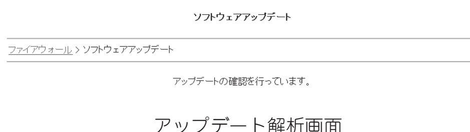
ユーザ認証が行われます。



ユーザ認証に失敗した場合には、ユーザ認証画面に戻ります。

ユーザ認証に成功すると、Express5800/SG300はあらかじめ定められたサイトと通信し、アップデート情報の取得をします。

配布可能なアップデート情報の一覧を示したアップデート画面が表示されます。



アップデート解析画面



［認証しない］をクリックした場合は、Express5800/SG300はあらかじめ定められたサイトと通信し、認証を経ていないユーザにも配布可能なアップデート情報を取得し、アップデート情報の一覧を示したアップデート画面を表示します。



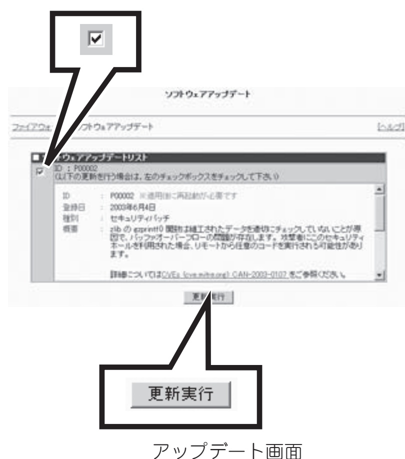
- サイトとの通信に失敗した場合は、エラー画面が表示されます。フィルタリング設定、プロキシの設定を確認してください。
- アップデートの必要がない場合は、「アップデート対象のソフトウェアはありません」画面が表示されます。[戻る]をクリックしてください。

6. アップデート画面において、適用したいアップデート情報のチェックボックスをチェックし、［更新実行］をクリックする。

選択したアップデート情報をExpress5800/SG300に適用します。

重要

アップデート情報の内容によっては、適用後すぐにシステムの再起動を必要とするものがあります。適用後すぐにシステムの再起動が必要な場合は[更新実行]をクリックすると、再起動実行の確認画面が表示されます。再起動しても問題がなければ[OK]をクリックしてください。

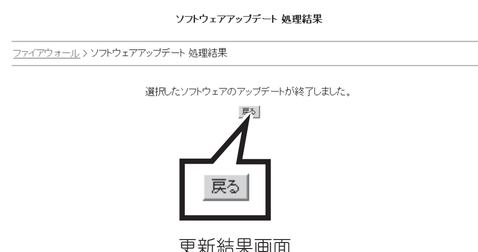


アップデート画面

アップデート情報の適用に成功すると更新結果画面が表示されます。

7. ［戻る］をクリックする。

ファイアウォールメニュー画面に戻ります。



更新結果画面

ヒント

適用後すぐにシステムの再起動が必要な更新の場合は、更新結果画面（システム再起動時）が表示され、システムの再起動が自動的に行われます。再起動したら再度Management Consoleにログインしてください。

なお、適用後すぐにシステムの再起動を必要とするアップデートは一度に1つのパッケージしか適用できません。複数のアップデート情報がある場合は、再度ソフトウェアアップデートの操作を行ってください。

チェック

ソフトウェアアップデートに失敗した場合は、エラー画面が表示されます。Express5800/SG300のソフトウェアの状態はアップデートを行う前の状態に戻ります。

バックアップ

万一の障害や災害に備え、管理者はExpress5800/SG300に設定したファイアウォールの各種情報を定期的にバックアップする必要があります。必要な時に保存しておいたバックアップデータをリストアすれば、バックアップを取得した時点の状態にExpress5800/SG300を戻すことができます。

バックアップの取得

バックアップには、ルールやグループ情報などのデータのバックアップを取得する方式と、ファイアウォール機能全体を通してのバックアップを取得する方式があります。

1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   ファイアウォールメニュー画面が表示されます。



2. ファイアウォールメニューの「システムメンテナンス」から[バックアップ・リストア]をクリックする。

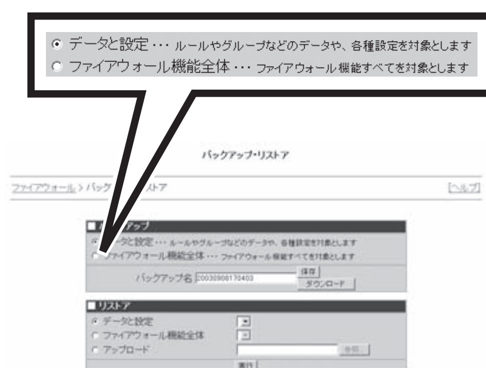
   バックアップ取得およびリストア画面が表示されます。



ファイアウォールメニュー画面

3. バックアップの方式を選択する。

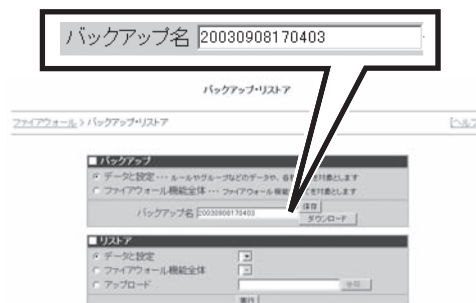
   - データと設定
     ファイアウォール機能の各種設定ファイルとデータベース情報を取得します。
   - ファイアウォール機能全体
     「データと設定」で取得するバックアップデータに加えて、システムの基本設定を除くファイアウォールコンポーネントのバイナリを取得します。



バックアップ・リストア画面

4. 「バックアップ名」を入力する。

   ここで入力した名前でバックアップデータは保存されます。

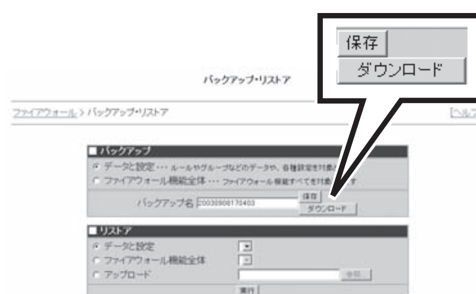


バックアップ・リストア画面

5. [保存]または[ダウンロード]をクリックする。

   - 保存
     取得したバックアップデータをExpress5800/SG300上に保存します。
   - ダウンロード
     取得したバックアップデータを管理者が操作する管理クライアント上に保存します。

   保存に成功すると、保存結果画面が表示されます。

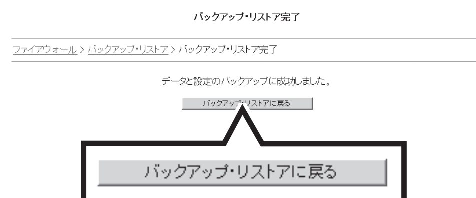


バックアップ・リストア画面



バックアップデータの取得に失敗した場合は、エラー内容を示す画面が表示されます。

6. [バックアップ・リストアに戻る]をクリックする。



バックアップ・リストア完了画面

バックアップのリストア

必要な時にバックアップデータをリストアすることで、Express5800/SG300をバックアップデータを取得した時点の状態に戻すことができます。

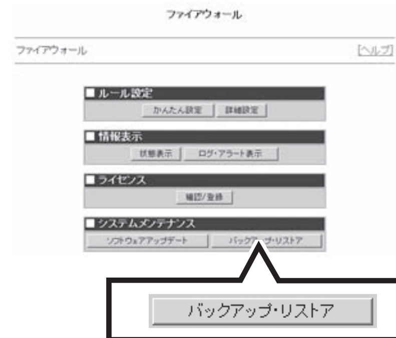
1. Management Consoleトップ画面の左側に表示されるメニューアイコンから[ファイアウォール]をクリックする。

   「ファイアウォール」メニュー画面が表示されます。



2. 「ファイアウォール」メニューの「システムメンテナンス」から[バックアップ・リストア]をクリックする。

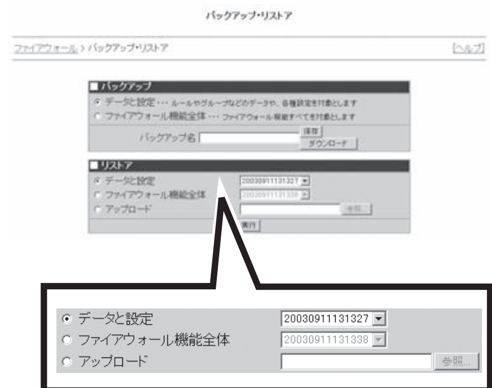
   バックアップ取得およびリストア画面が表示されます。



ファイアウォールメニュー画面

3. リストアするバックアップデータを選択する。

   - データと設定
     ファイアウォール機能の各種設定ファイルとデータベース情報をリストアします。
   - ファイアウォール機能全体
     「データと設定」で取得するバックアップデータに加えて、システムの基本設定を除くファイアウォールコンポーネントのバイナリをリストアします。
   - アップロード
     管理者が操作する管理クライアント上に保存したバックアップデータをリストアします。



バックアップ・リストア画面

4. 「データと設定」、「ファイアウォール機能全体」を選択した場合は、バックアップデータの名前をプルダウンメニューから選択し、「アップロード」を選択した場合は入力フィールドに入力することで、リストアするバックアップデータを指定する。



入力フィールドに入力する場合、[参照]をクリックしてデータを指定することもできます。



管理クライアント上に取得したバックアップデータをリストアする場合は、「データと設定」に含まれるバックアップデータをリストアするか、「ファイアウォール機能全体」に含まれるバックアップデータをリストアするのかは、Express5800/SG300が自動的に判別するため、指定する必要はありません。

バックアップ・リストア画面

5. ［実行］をクリックする。

バックアップデータのリストアが実行され完了すると、リストア結果画面が表示されます。



リストアに失敗した場合は、エラー内容を示す画面を表示します。

バックアップ・リストア画面

6. ［バックアップ・リストアに戻る］をクリックする。

バックアップ・リストア完了画面

ユーザ認証

ここでは、ユーザが端末からExpress5800/SG300を越えて通信を行う場合のユーザ認証について説明します。

ユーザ認証

かんたん設定ウィザードまたは認証設定で「ユーザ認証を利用する」と設定した場合、ユーザ認証機能を利用できるようになります。ユーザ認証機能を利用した場合、ユーザごとのアクセス制御が可能になります。かんたん設定ウィザードについては、95ページの「かんたん設定ウィザード」を、「認証設定」については227ページを参照してください。ここでは、ユーザのログイン操作について説明します。

1. ブラウザで、Express5800/SG300が持つIPアドレスを、「https://」に続けて指定する。



かんたん設定の「ユーザ認証の利用の設定」で、「内部ネットワークからのみ許可する」を選択している場合は、Express5800/SG300が持つ内部ネットワークに属するIPアドレスを指定する必要があります。またこの場合、アクセス元は内部ネットワークからである必要があります。

2. 上記URLに続けてユーザ認証のウェブのポート番号を指定する。

このポート番号は、かんたん設定ウィザードで設定したものを指定します。

例）　https://202.247.5.126:443

ポート番号

外部インタフェースのIPアドレス



ポート番号が443番（デフォルト設定）の場合は、番号を省略することが可能です。

ユーザログイン画面が表示されます。

ファイアウォール機能の設定方法

3. 画面に従い「ユーザID」、「パスワード」を入力し、[ログイン]ボタンをクリックする。

認証要求がExpress5800/SG300に送られ、Express5800/SG300は自身が管理するユーザ情報と照らし合わせて、正しいユーザによるログインであるか認証します。

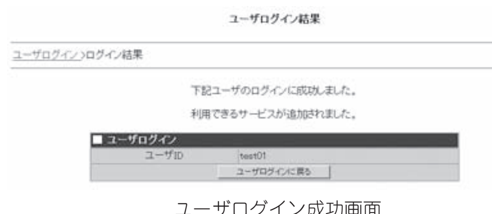


ユーザログイン画面

正しいユーザであることが認証されると、ユーザログイン成功画面が表示されます。



誤ったユーザID、またはパスワードを送信した場合は、認証が失敗したことを示す画面が表示されます。認証に繰り返し失敗したユーザアカウントは、自動的にロックアウトします。許容する単位時間あたりの失敗回数、およびロックアウトの継続時間については、229ページの「ロックアウト設定」を参照してください。



ユーザログイン成功画面



ユーザが所属するグループのルールが設定されている場合、ユーザログインに成功すると、グループルールが有効化されます。有効化されたルールは、そのユーザのセッションが終了したとしても、そのルールに定められた有効期限の間、適用されたままとなります。

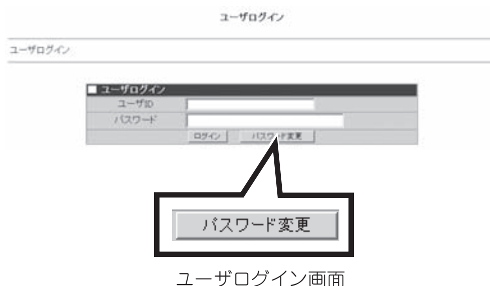
ユーザパスワードの変更

ユーザログイン画面からパスワードを変更することができます。ここでは、ユーザが各自のパスワードを変更する操作について説明します。

1. URLおよびポート番号を指定し、ユーザログイン画面を表示させる。

2. ユーザID、パスワードを入力し、［パスワード変更］をクリックする。

   ユーザパスワード変更画面が表示されます。



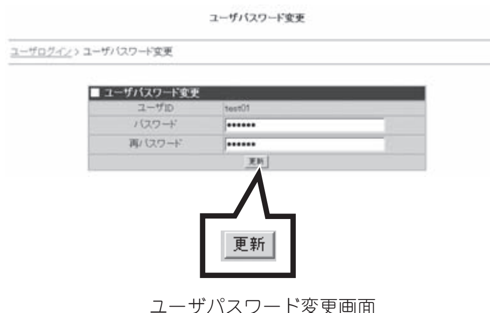
ユーザログイン画面

3. 「パスワード」、「再パスワード」に新しいパスワードを入力し、［更新］をクリックする。

   Express5800/SG300が新しいパスワードデータを受け取ると、管理しているユーザ情報において該当ユーザのパスワード情報の更新を行います。パスワードの変更に成功した場合は、ユーザの端末にパスワード変更成功画面を表示します。



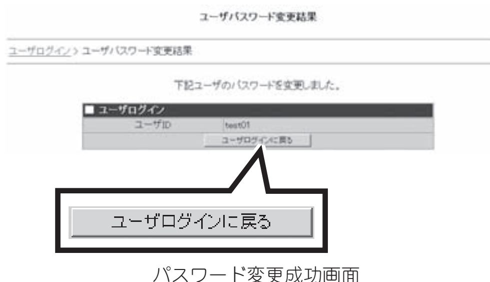
パスワード変更に失敗した場合は、変更に失敗したことを示す画面を表示します。



ユーザパスワード変更画面

4. ［ユーザログインに戻る］をクリックする。

   ユーザログイン画面が表示されます。新しいパスワードでログインしてください。



パスワード変更成功画面

~Memo~